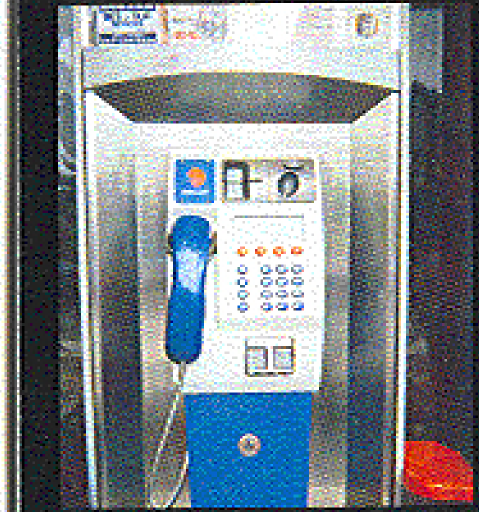
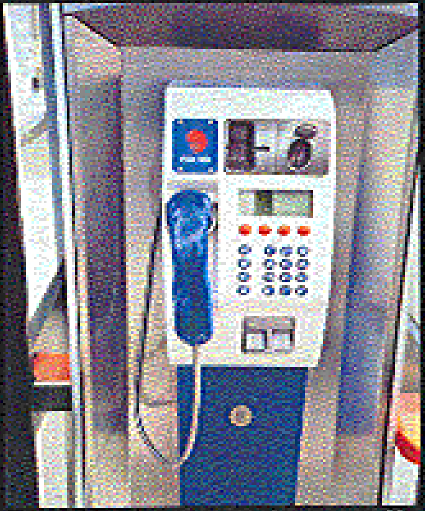
Irish Payphones



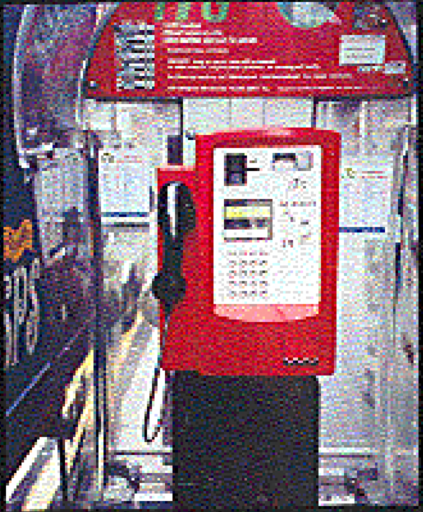
From Cong in County Mayo of the **Irish** Republic, a card/coin model operated by Eircom.

Photo by Jamie Stack



This could be the same exact phone captured by an entirely different person. But we doubt it.

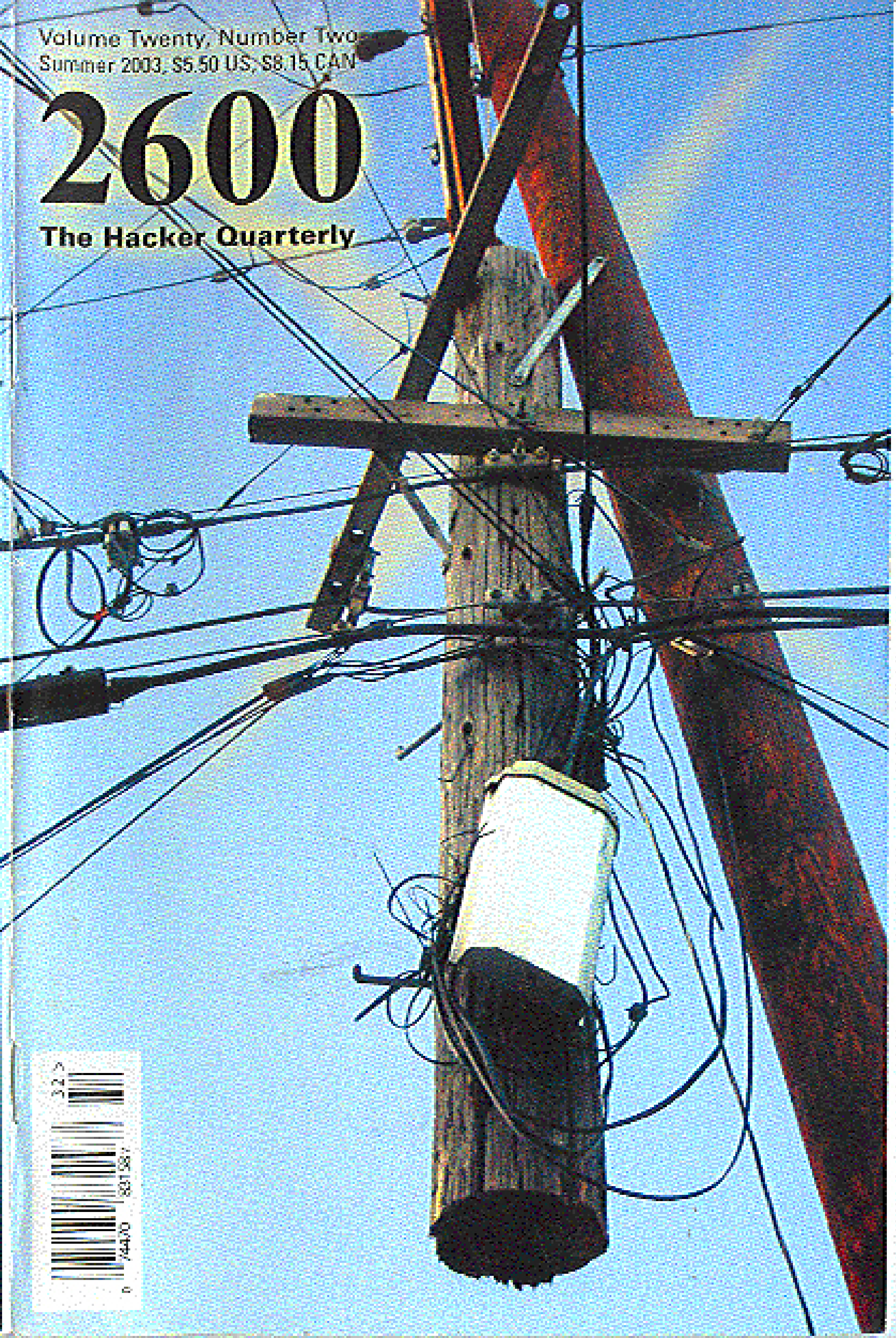
An outer view of the booth of the previous phone(s).



An entirely different type of phone from a different company known as ITG, whose phones can be found across the British Isles.

Photos by Raul Perez

Look on the other side of this page for even more photos!



Volume Twenty, Number Two
Summer 2003, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly

"Television taught people to watch 'Friends' rather than have friends. Today, relatively little of our leisure time is spent interacting with other people. Now we spend it observing machines."
- Robert B. Putnam,
author of *Bowling Alone*

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Photo
David Buchwald

Cover Design
Mike Essl

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dalal, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, David Ruderman, Screamer Chaotix, Seraf, Silent Switchman, Mr. Upsetter

Webmasters: Juintz, Kerry

Network Operations: css, mlc, Seraf

Broadcast Coordinators: Juintz, Pete, daRonin, Digital Mercenary, Kobold, w3rd, Gehenna, Brilldon, Chibi-Kim, lee, Nico, Logix, Boink, John

IRC Admins: Antipent, daRonin, Digital Mercenary, Redhackt, Roadie, Shardy, The Electronic Delinquent

Inspirational Music: Donovan, The Evolution Control Committee, Sparks, Cheap Trick, Gang of Four

Shout Outs: George, Brian, Chub, Pete, Mike, Joe Two Rivers

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 2 Flowerfield, St. James, NY 11780. Second class postage permit paid at Setauket, New York.

POSTMASTER:
Send address changes to
2600, P.O. Box 752, Middle Island,
NY 11953-0752.

Yearly subscription: U.S. and Canada - $20 individual, $50 corporate (U.S. funds). Overseas - $30 individual, $65 corporate. Back issues available for 1984-2002 at $20 per year, $25 per year overseas. Individual issues available from 1988 on at $5.50 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752
(subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 Office Line: 631-751-2600
2600 FAX Line: 631-474-2677

Junk

Disrespecting the Law

Over and over, we're told that above all else we must respect the law. Whether or not we disagree with it, whether or not we feel it's unfair, even when just about everybody *knows* it's a bad law, the one thing that's always been made clear to us is that the law is the law. So it's especially telling when we see just how little the law actually means to lawmakers and those in power.

There is a process by which injustices can be corrected. It's rarely quick and easy and it usually involves a good amount of sacrifice on the part of those trying to change the way things are. The abolition of slavery, women's suffrage, the civil rights movement, even some changes in the foreign policy of the U.S. government came about as a result of intense lobbying, massive demonstrations, and people willing to give up everything in order to stand up for something they believed in.

We see this today on a number of fronts that affect us quite directly, not the least of which is the Digital Millennium Copyright Act (DMCA), used to prosecute *2600* back in 2000. While we lost that fight, the battle against the DMCA continues to this day and we are committed to overturning an unjust law that has robbed many of basic freedoms in the world of digital technology. What laws like the Patriot Act have done to our country is so frightening as to be almost unbelievable. But there are millions of people determined to fight back and attempt to keep civil rights from crumbling into dust.

Disobeying an unjust law is another tactic to force the hand of the lawmakers, one which often carries a heavy price. Despite this, it's rare that the entire structure of the legal system is also disobeyed - those engaging in civil disobedience tend not to try and escape prosecution; rather, they use the structure of the system to voice their objections to the law or policy they're protesting against.

But now we are at a point where those already in power have grown impatient with such things as due process, civil rights, and public perception. In some disturbing and almost comical examples, we see exactly how little the law actually means to them.

Senator Orrin Hatch (R-Utah) has been involved in discussions with a company called MediaDefender which has developed a product to disrupt music downloads (yes, that's what they do). In a recent exchange, Hatch expressed his interest in "destroying" the computers of those suspected of copyright violation. In his words, such an act "may be the only way you can teach somebody about copyrights." This isn't some drunkard in a bar offering a completely insane solution to a problem. This is a United States Senator.

And it's not the first time we've heard this kind of talk. The Recording Industry Association of America (RIAA) has in the past tried to get legislation passed that would allow copyright holders to hack into the computers of people suspected of having music that they didn't pay for. In fact, they attempted to tack this onto an anti-terrorism bill, no doubt hoping that the hysteria of the moment would keep their blatant attempt to bypass due process unnoticed. Fortunately, it didn't work - that time.

Then, in 2002, right before the August recess, Rep. Howard Berman (D-California) proposed another bill to do basically the same thing. '"No legislation can eradicate the problem of peer-to-peer piracy. However, enabling copyright creators to take action to prevent an infringing file from being shared via P2P (peer-to-peer) is an important first step," he said.

There was only one problem. To do what they wanted was illegal under all kinds of laws. So part of what this bill was pushing for was immunity from prosecution. That means the MPAA and RIAA could completely disable, block, and even damage a publicly accessible network if they believed something they didn't like was going on there. And anyone whose computer was damaged as a result of this would have to get *permission* from the U.S. attorney general to sue the perpetrators and then only if the damages were above $250!

New life may be breathed into this legislation by Hatch's recent comments. He said that the system he envisioned would warn a computer user twice if they were doing something objectionable and "then destroy their computer."

"If that's the only way, then I'm all for destroying their machines," he went on to say.

In a civilized society, laws exist for a reason. At least in theory, they are designed to provide a level playing field and a chance of equal justice for one and all. Individuals break laws for a variety of reasons, usually either to gain an advantage or to recover from a disadvantage. But when governments break these laws, it's because they fear losing control. They begin to act with desperation and start to lose touch with reality. We've seen this all before in many parts of the world throughout history.

Over the past couple of years, we've been witness to this sort of thing on a much larger scale. Civil liberties have become dirty words. The Freedom of Information Act is practically a thing of the past. People who question policy are accused of being traitors. And fear, always the most essential ingredient in such a downward spiral, has become an omnipresent part of our daily lives.

It's always the feeling of crisis which permits what would otherwise be unacceptable changes to practically be welcomed by the public. And, since these changes are unlikely ever to be reversed, society is forever changed in a very negative way.

It would have been completely unheard of only two years ago for people here to be rounded into prison camps and held without charge or without even confirmation of their detention. It happens today and it's no longer even in the news. Most of the time these people aren't citizens of the United States, which in itself is enough to make most of us not care. The fact that someone could be held without charges, bail, or even the right to communicate with their family because of a minor visa violation is overlooked because it's all part of the fight against terrorism and certain laws and basic rights need to be overlooked because they just got in the way.

But there are now increasing examples of U.S. citizens being affected by this as well, such as the case of former Intel software engineer Mike Hawash, held without charges for five weeks and now scheduled to go on trial next January for "Conspiracy to Levy War on the United States." Only extremely sketchy information has been given by the government and it's not likely any more will be released before his trial. (More information can be found at http://www.freemikehawash.org.)

By being defined as an "enemy combatant," the rules on due process can be suspended. Not only that but torture is increasingly seen as a valid way of obtaining information from a suspect. Eventually, people will come to embrace such things in the mistaken belief that their world is being made more secure.

The arrogance and disrespect towards laws and values that have taken centuries to shape doesn't confine itself to within our borders. The recent military aggressions of our nation have only reinforced the impression that the American government merely tolerates laws and treaties until they become inconvenient. In the end, it does whatever it wants to do.

This now includes assassination of foreign leaders, preemptive invasion of any country which *may* someday pose a risk to ours, "punishing" any allies who refuse to go along, and, perhaps most telling, steadfastly refusing to be answerable to the International Criminal Court (although the United States and 138 other countries had already signed on). Congress even went so far as to pass a law authorizing the invasion of The Netherlands to free any U.S. serviceman accused of a war crime! (The ICC is located in The Hague.) Such a violent reaction to even the mere possibility that our soldiers could be held accountable for war crimes has alienated the United States even more.

A government that fails to respect its laws will eventually lose the confidence of its citizens. And a country that fails to respect international law will be looked down upon by the rest of the world and, one way or another, isolated. The two combined is a frightening prospect, especially given our "superpower" status.

Those who feel that existing laws are an inconvenience to their agenda do not have the right to exempt themselves from their power. Like the individuals who challenge the worthiness of a law, there are but two choices - either challenge that effectiveness through courts, public demonstrations, etc. or disobey them and pay the price, using that process as a tool to promote change. If we permit those with power to continue this pattern of choosing which laws apply to them and which apply to everyone else, we will soon have very little worth fighting for.

ROLL YOUR OWN

iis intrusion detection system

by The Rev. Dr. Jackal-Headed-God

If you're in the web development profession and get as many free professional subscriptions as I do, you will notice that at least once per year, each magazine will run a special edition on hacking. Usually there's some sort of catchy cover image showing a shady character engaged in symbolically nefarious behavior. Inside, you'll read about the latest worms, viruses, and "hacks" that your mission-critical web site might be susceptible to. Then you'll read reviews of the latest web site security software, gasp at the cost, and then either try to convince your boss to open her wallet or just move on. It's the standard marketing tactic of scaring you into busting your budget.

So it's a given that there are plenty of top-shelf web security solutions out there. It's also a given that none of them is perfect. And, of course, almost all of them come with a hefty price tag.

This article will show you how to roll your own intrusion detection system for Microsoft's Internet Information Server (IIS) - one that's absolutely free, 200 lines of code, and about 90 percent effective. It assumes that you are running IIS 5.x on Windows 2000, with ActiveState Perl installed (free from www.activestate.com) and configured to run CGI scripts. See ActiveState's documentation on how to set this up. (Hint: don't forget to map .cgi to the Perl interpreter; by default, only .pl is mapped. Sloppy.)

Attack of the Script Kiddies

So what happens when someone decides to target your web site for an attack? Typically, the would-be intruder will use the script kiddy tool de jour, which will scan the target site for a laundry list of well-known vulnerabilities. After the initial scan, the tool will come back with specific vulnerabilities and wait for the order to exploit them. This is analogous to walking around a house and loudly knocking on all the doors and windows, looking for one that's unlocked.

What we're going to focus on is not how to avoid vulnerabilities (read cert.org daily, keep up with vendor patches, be alert, etc.), but rather on how to take advantage of your server's invulnerabilities. We'll listen for that knock and answer it.

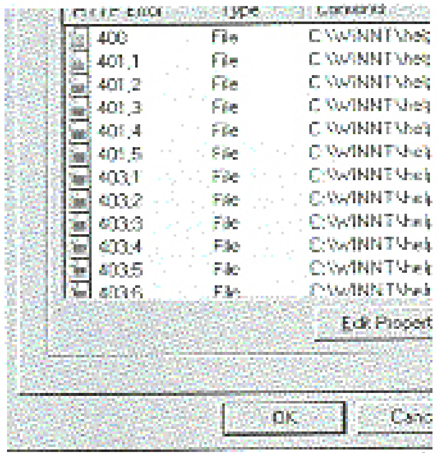
How IIS Handles Server Errors

What happens to all of the exploit tests that fail? Usually, they generate server errors (403 Access Forbidden, 400 Bad Request, or 500 Server Error). These server errors are duly noted in your web server's error log and are never, ever noticed. Why? Because no one looks at error logs, of course. And if they do, it's usually too late.

In addition to writing an entry in the error log, IIS will also display a page to the user informing them that an error has occurred. These canned error responses (there are about 60 of them) can be found by default in C:\WINNT\Help\iisHelp\common. Take a look; you'll find one .htm file for each kind of error that IIS understands.

Overriding Default Error Handling

Fire up Internet Services Manager on your web server (usually under Administrative Tools in the Start menu). Right-click on your web site, click on Properties, and select the "Custom Errors" tab. You should see something like this:



HTTP Error	Type	Contents
400	File	C:\WINNT\hel
401,1	File	C:\WINNT\hel
401,2	File	C:\WINNT\hel
401,3	File	C:\WINNT\hel
401,4	File	C:\WINNT\hel
401,5	File	C:\WINNT\hel
403,1	File	C:\WINNT\hel
403,2	File	C:\WINNT\hel
403,3	File	C:\WINNT\hel
403,4	File	C:\WINNT\hel
403,5	File	C:\WINNT\hel
403,6	File	C:\WINNT\hel

You can see that each HTTP error is mapped to an .htm file, the same files that you found in the iisHelp directory. These pages do a fine job of informing the end user that Something Bad Has Happened, but they don't do a thing to alert the system administrator. Let's fix that.

Introducing Watcher

Watcher is a very simple, 200-line Perl script that watches for suspicious server errors and lets you know about them. The source should be dropped in an appropriate folder on your web server inside the web root. Let's see what it does.

The program opens with the standard #!/usr/bin/perl header - not necessary in the Windows world, but UNIX habits die hard.

Configuration lines go first. We start with the address for the main recipient for e-mail alerts. Note that the @ is escaped with a backslash. Forget this, and you'll blow the script up. Next is a list of additional addresses for cc: notification.

SMTP (Simple Mail Transfer Protocol) server information is next. The smtpServerName variable is set to the IP address of an available SMTP server on your network. This server needs to be able to send mail to the outside world. The smtpPickupPath variable is the path to a specific folder on the box that the SMTP server watches for new outgoing mail. By default, it's c:\\inetpub\\mailroot\\pickup\\. Note the double backslashes.

Finally, we have a list of HTTP errors that we want to watch out for. The default list should cover all the more interesting situations, but feel free to customize it if you want. If you're observant, you'll notice an error code that doesn't belong: 1013. This will be our catch-all for those server errors that IIS doesn't know how to handle.

There are four subroutines.

We're going to make IIS pass us the specific HTTP error code through the path, so the first subroutine (getError) simply extracts this information from the URL.

getDateTime does just that - grabs the current date and time and formats it for easier reading. Most web servers use Greenwich Mean Time, so we'll subtract six hours (21600 seconds) from the time to convert to Central time. You can do the math to modify this line for your local time zone.

returnHTML handles the user-friendly error message that is returned to the browser when the error occurs. You can customize the HTML in this subroutine to display whatever you want.

Finally, writeMail gathers information about the server, the error, and the browser that caused the error and compiles it into an e-mail message. This file is then dropped into your SMTP server's pickup directory and you get an e-mail warning that something's happening on your server.

To configure IIS to use the Watcher script to handle server errors, go back into Internet Services Manager, select Properties for your web site, and go back to the Custom Errors tab. Double click on each entry that corresponds to the %errors code that you found in the Watcher script. Change the Message Type to URL. In the URL field, enter the relative URL to the Watcher script (e.g. /cgi/watcher.cgi). Hit OK, hit Apply, and stop and start your web site just for good measure.

To test your configuration, start off by just applying the change to error code 404. Modify the @trigger list to include 404 as a mail-triggering condition. Then fire up a browser, point it to your web site, and request a page that doesn't exist (e.g. foo.htm).

If your test was successful, you should see the error page from the Watcher script come up in your browser, and you should have an e-mail in your inbox. (Make sure that you remove 404 from the @trigger list.) If you don't see the error page, you either didn't put the correct URL in the error mapping dialog box, you don't have permissions set up on your cgi directory, you forgot to map .cgi to the Perl interpreter, or you otherwise didn't follow instructions. If you don't receive an e-mail, make sure that you put in the correct e-mail address, that your SMTP server is set up properly, and that you mapped to the correct SMTP pickup directory. Beyond that, I'll have to leave it to you to figure out what you did wrong.

Spring Forward

Among the information that you receive by mail is the software used to access your site (usually a web browser, but sometimes an automated script), the bad HTTP request that generated the error, and the IP address of the would-be intruder. Here's a sample, with IP addresses x'ed out for the sake of liability:

```
A server error occurred on 3/8/2003 at 1:27 am
CST. Details below.
---------------------------------------------------
This error message was returned to the user:

Access Forbidden (403)

Access to this URL is not allowed. Please use the
'Back' button on your browser.
---------------------------------------------------

REQUEST INFO
---------------
Referrer:
Request:
http://xxx.xxx.93.10/_vti_cnf/..%255c..%255c..%
    255c..%255c..%255c..%255cwinnt/system32/
        cmd.exe?/c+dir+c:\
Query String:
403;http://xxx.xxx.93.10/_vti_cnf/..%255c..%255c.
    .%255c..%255c..%255c..%255cwinnt/system32
        /cmd.exe?/c+dir+c:\
Method: HEAD
Port: 80
Protocol: HTTP/1.0


USER INFO
---------------
Remote address: xx.130.93.214
Remote host: xx.130.93.214
User Agent:
Remote Ident:
Remote User:
Authorization Type:


RESPONSE INFO
---------------
Script name: /errors/httperror.cgi
Content Length: 26791
Content Type: text/html
Path Info: /errors/httperror.cgi
Translated Path: C:\webroot\somesite\cgi\watcher.cgi
```

```
SERVER INFO
---------------
Server Name: xxx.xxx.93.10
Computer Name: SOMESERVER
Gateway Interface: CGI/1.1
Server Software: Microsoft-IIS/5.0
System Drive: C:
System Root: C:\WINNT
Windows Directory: C:\WINNT
User Profile: C:\Documents and Settings\ComProdSvc
Path: C:\Perl\bin\;C:\WINNT\system32;C:\
    WINNT;C:\WINNT\System32\Wbem;C:\
        WINNT\System32\WBEM;C:\WINNT\
            System32\WBEM\SNMP
```

Notice what's in the Request line under REQUEST INFO. Why, it's someone attempting a Unicode Directory Traversal exploit. Gotcha.

You can use the user profile information to do a traceroute on the "Remote Address" IP address to find out where the attack is coming from. Next I recommend using whois.bw.org to find out who owns the IP. Collect everything you'll need later, because odds are they won't be around for long. Get on the phone with your provider (or your MIS staff) to block all traffic from the subnet of the attacker while you portscan the miscreant and, um, do whatever you feel is justified. (Hint to all script kiddies: make sure your box is secure before you go hunting for exploits.)

Room for Improvement

Watcher is a passive tool, very simple to implement, that will give you an early warning with just about every clumsy attempt to find and exploit a vulnerability in your IIS-based web site. Having said that, there is a lot of room for improvement. For one thing, when your site does come under attack, you're going to get a lot of e-mail. Any Perl hacker worth his salt could extend Watcher to throttle the number of e-mails that it will send in a given period of time. Logging all suspicious activity to a file wouldn't hurt either. And many worms, viruses, and exploits leave a signature - like that garbage in the Request line we saw earlier - that can be used to identify the type of attack that is being attempted.

I've kept Watcher simple and clean for the sake of this article, but once you get familiar with the concept, there's a lot that you can do to extend it to suit your particular needs. Best of all, you don't have to beg your boss to pay for it - it's free.

```
#           Watcher.cgi
#           A passive Intrusion Detection tool
#           Written by The Rev. Dr. Jackal-Headed-God

#           Configuration stuff

            $recipient = "admin\@myisp.com";
            @cclist = ("someone\@myisp.com","someone.else\@myisp.com");
            $smtp_server_name = "xxx.xxx.145.9";
            $smtp_pickup_path = "c:\\inetpub\\mailroot\\pickup\\";
            $errorCode = "1111";   # Catch-all error code
            $request = "unknown_error"; # Catch all code past desc

            # What HTTP errors should trigger an e-mail alert?

            @mailtrigger = ("400","401","404","405","406","407","412","414","500","501","1111");

            # Error codes and descriptions returned to the user.

            %errors = (

                        "400" => "Bad Request|Due to malformed syntax, the request could not be understood by
the server. The client should not repeat the request without modifications.",

                        "401" => "Unauthorized. Logon Failed|This error indicates that the credentials passed
to the server do not match the credentials required to log on to the server. Please contact the Web server's
administrator to verify that you have permission to access the requested resource.",

                        "401.1" => "Unauthorized: Logon Failed|This error indicates that the credentials
passed to the server do not match the credentials required to log on to the server. Please contact the Web
server's administrator to verify that you have permission to access the requested resource.",

                        "401.2" => "Unauthorized. Logon Failed due to server configuration|This error
indicates that the credentials passed to the server do not match the credentials required to log on to the
server. This is usually caused by not sending the proper WWW-Authenticate header field. Please contact the
Web server's administrator to verify that you have permission to access to requested resource.",

                        "401.3" => "Unauthorized: Unauthorized due to ACL on resource|This error indicates
that the credentials passed by the client do not have access to the particular resource on the server. This
resource could be either the page or file listed in the address line of the client, or it could be another
file on the server that is needed to process the file listed on the address line of the client. Please make a
note of the entire address you were trying to access and then contact the Web server's administrator to ver-
ify that you have permission to access the requested resource.",

                        "401.4" => "Unauthorized. Authorization failed by filter|This error indicates that the
Web server has a filter program installed to verify users connecting to the server. The authentication used
to connect to the server was denied access by this filter program. Please make a note of the entire address
you were trying to access and then contact the Web server's administrator to verify that you have permission
to access the requested resource.",

                        "401.5" => "Unauthorized. Authorization failed by ISAPI/CGI app|This error indicates
that the address on the Web server you attempted to use has an ISAPI or CGI program installed that verifies
user credentials before proceeding. The authentication used to connect to the server was denied access by
this program. Please make a note of the entire address you were trying to access and then contact the Web
server's administrator to verify that you have permission to access the requested resource.",

                        "404" => "Access Forbidden|Access to this URL is not allowed. Please use the 'Back'
button on your browser, or select a link from the navigation sidebar to the left.",

                        "403.1" => "Forbidden: Execute Access Forbidden|This error can be caused if you try to
execute a CGI, ISAPI, or other executable program from a directory that does not allow programs to be exe-
cuted. Please contact the Web server's administrator if the problem persists.",

                        "403.10" => "Access Forbidden: Invalid Configuration|There is a configuration problem on
the Web server at this time. Please contact the Web server's administrator if the problem persists.",

                        "403.11" => "Access Forbidden. Password Change|This error can be caused if the user
has entered the wrong password during authentication. Please refresh the page and try again. Please contact
the Web server's administrator if the problem persists.",

                        "403.12" => "Access Forbidden. Mapper Denied Access|Your client certificate map has
been denied access to this Web site. Please contact the site administrator to establish client certificate
permissions. You can also change your client certificate and retry, if appropriate.",

                        "403.2" => "Forbidden. Read Access Forbidden|This error can be caused if there is no
default page available and directory browsing has not been enabled for the directory, or if you are trying
to display an HTML page that resides in a directory marked for Execute or Script permissions only. Please
contact the Web server's administrator if the problem persists.",

                        "403.3" => "Forbidden: Write Access Forbidden|This error can be caused if you attempt
to upload to, or modify a file in, a directory that does not allow Write access. Please contact the Web
server's administrator if the problem persists.",

                        "403.4" => "Forbidden: SSL required|This error indicates that the page you are trying
to access is secured with Secure Sockets Layer (SSL).  In order to view it, you need to enable SSL by typing
"https://" at the beginning of the address you are attempting to reach. Please contact the Web server's
administrator if the problem persists.",

                        "403.5" => "Forbidden: SSL 128 required|This error message indicates that the resource
you are trying to access is secured with a 128-bit version of Secure Sockets Layer (SSL). In order to view
this resource, you need a browser that supports this level of SSL. Please confirm that your browser supports
128 bit SSL security. If it does, then contact the Web server's administrator and report the problem.",

                        "403.6" => "Forbidden. IP address rejected|This error is caused when the server has a
list of IP addresses that are not allowed to access the site, and the IP address you are using is in this
list.  Please contact the Web server's administrator if the problem persists.",

                        "403.7" => "Forbidden: Client certificate required|This error occurs when the resource
you are attempting to access requires your browser to have a client Secure Sockets Layer (SSL) certificate
that the server recognizes. This is used for authenticating you as a valid user of the resource. Please
contact the Web server's administrator to obtain a valid client certificate.",

                        "403.8" => "Forbidden: Site access denied|This error can be caused if the Web server
is not servicing requests, or if you do not have permission to connect to the site. Please contact the Web
server's administrator.",

                        "403.9" => "Access Forbidden: Too many users are connected|This error can be caused if
the Web server is busy and cannot process your request due to heavy traffic. Please try to connect again
later. Please contact the Web server's administrator if the problem persists.",

                        "403.14" => "Access Forbidden|Directory listings are not allowed. Please use the
'Back' button on your browser, or select a link from the navigation sidebar to the left.",

                        "404" => "Page Not Found|The server could not locate the page that you requested.",

                        "405" => "Method Not Allowed|The method specified in the Request Line is not allowed
for the resource identified by the request. Please ensure that you have the proper MIME type set up for the
resource you are requesting. Please contact the server's administrator if this problem persists.",

                        "406" => "Not Acceptable|The resource identified by the request can only generate re-
sponse entities that have content characteristics that are 'not acceptable' according to the Accept headers
sent in the request. Please contact the server's administrator if this problem persists.",

                        "407" => "Proxy Authentication Required|You must authenticate with a proxy server
before this request can be serviced.  Please log on to your proxy server, and then try again. Please contact
the Web server's administrator if this problem persists.",

                        "412" => "Precondition Failed|The precondition given in one or more of the Request-
header fields evaluated to FALSE when it was tested on the server. The client placed preconditions on the
current resource metainformation (header field data) to prevent the requested method from being applied to a
resource other than the one intended. Please contact the Web server's administrator if the problem persists.",
                        "414" => "Request URI Too Long|The server is refusing to service the request because
the Request-URI is too long. This rare condition is likely to occur only in the following situations:",

                        "500" => "Internal Server Error|The Web server is incapable of performing the request.
Please try your request again later. Please contact the Web server's administrator if this problem per
sists.",

                        "501" => "Not Implemented|The Web server does not support the functionality required
to fulfill the request. Please check your URL for errors, and contact the Web server's administrator if the
problem persists.",

                        "502" => "Bad Gateway|The server, while acting as a gateway or proxy, received an in
valid response from the upstream server it accessed in attempting to fulfill the request. Please contact the
Web server's administrator if the problem persists.",

                        "1013" => "Something Bizarre Just Happened|A truly bizarre error has occurred. I have
no idea what you just did, but I'll certainly try to figure it out."

            );

            &getError;
            &getDateTime;
            &returnHTML;
            &writeMail;

#           Subroutines

sub getError {

            if ($ENV{'QUERY_STRING'}) { ($ErrorCode, $request) = split /;/, $ENV{'QUERY_STRING'},2; }
            $ErrorName = $Errors{$ErrorCode};
            $ErrorName =~ s/\|.*//;
            $ErrorDesc = $Errors{$ErrorCode};
            $ErrorDesc =~ s/.*\|//;
}

sub getDateTime {

            my ($sec,$min,$hour,$mday,$mon,$year,$wday) = gmtime(time-21600); # GMT - 6 hours (in seconds) = CST
            my $ampm;
            my $zformat;
            $year = 1900 + $year;
            if ($min < 10) { $min = "0$min"; }
            if ($sec < 10) { $sec = "0$sec"; }
            if ($hour < 12) { $ampm = "am"; } else { $ampm = "pm"; }
            if ($hour > 12) { $hour = ($hour - 12); }
            if ($hour eq "0") { $hour = "12";}
            $datetime = ($mon + 1) . "\/$mday\/$year at $hour:$min $ampm CST";
}

sub returnHTML {

            print "Content-type: text/html\n\n";
            print <<"  EOF";

                        <html>
                        <head>
                        <meta name="robots" content="noindex">
                        <title>Error: Server Error $ErrorCode</title>
                        </head>
                        <body bgcolor="#FFFFFF">
                        <br><br>
                        <blockquote>
                        <p>An error has occurred. Details are provided below:</p>
                        <table border="0" cellspacing="0" cellpadding="1" bgcolor="#000000">
                        <tr>
                        <td valign="top" width="100%">
                        <table border="0" cellspacing="0" cellpadding="10" bgcolor="#eeeeee">
                        <tr>
                        <td valign="top" width="100%">
                        <p><b>$ErrorName [$ErrorCode]</b><br><br><font color="#000000">$ErrorDesc</font></b></p>
                        </td>
                        </tr>
                        </table>
                        </td>
                        </tr>
                        </table>
                        <br>

                        <p>If you continue having difficulties, please contact the webmaster.
                             Be sure to specify the error code [$ErrorCode] and the page you were trying to
                                  access [$request].</p>
                        </blockquote>
                        </body>
```

```
                        </html>

            EOF
}

sub writeMail {

            # First, check the list of trigger errors

            my $found;
            foreach my $TriggerCode (@mailtrigger) { if ($ErrorCode eq $TriggerCode) { $found = "true"; last; } }

            # If this error condition is in our trigger list, send an e-mail warning

            if ($found eq "true") {

                        my $server_name = lc($ENV{'COMPUTERNAME'});
                        my $from_name = "$server_name Watcher";
                        my $from_email = "$server_name\@mydomain.com";
                        my $subject = "$server_name\@mydomain.com Server Error [$ErrorCode $ErrorName]";
                        $tempfile = "watcher_$$.txt";

                        open TMP, ">$smtp_pickup_path$tempfile" or die;
                        print TMP "x-sender: $from_email\n";
                        print TMP "x-receiver: $recipient\n";
                        if (@cclist) { foreach my $ccaddress (@cclist) { print TMP "x-receiver: $ccaddress\n"; } }

                        print TMP "To: $recipient\n";
                        print TMP "CC: @cclist\n";
                        print TMP "From: $from_name <$from_email>\n";
                        print TMP "Subject: $subject\n";
                        print TMP "\n\n";
                        print TMP "A server error occurred on $datetime. Details below.\n";

                        print TMP "----------------------------------------------------------------------------\n";
                        print TMP "This error message was returned to the user:\n\n";
                        print TMP "$ErrorName [$ErrorCode]\n\n$ErrorDesc\n";
                        print TMP "----------------------------------------------------------------------------\n";
                        print TMP "\nREQUEST INFO\n----------------\n";
                        print TMP "Referrer: $ENV{'HTTP_REFERER'}\n";
                        print TMP "Request: $request\n";
                        print TMP "Query String: $ENV{'QUERY_STRING'}\n";
                        print TMP "Method: $ENV{'REQUEST_METHOD'}\n";
                        print TMP "Port: $ENV{'SERVER_PORT'}\n";
                        print TMP "Protocol: $ENV{'SERVER_PROTOCOL'}\n";
                        print TMP "\n\n";
                        print TMP "\nUSER INFO\n----------------\n";
                        print TMP "Remote Address: $ENV{'REMOTE_ADDR'}\n";
                        print TMP "Remote Host: $ENV{'REMOTE_HOST'}\n";
                        print TMP "User Agent: $ENV{'HTTP_USER_AGENT'}\n";
                        print TMP "Remote Ident: $ENV{'REMOTE_IDENT'}\n";
                        print TMP "Remote User: $ENV{'REMOTE_USER'}\n";
                        print TMP "Authentication Type: $ENV{'AUTH_TYPE'}\n";
                        print TMP "\n\n";
                        print TMP "\nRESPONSE INFO\n----------------\n";
                        print TMP "Script Name: $ENV{'SCRIPT_NAME'}\n";
                        print TMP "Content Length: $ENV{'CONTENT_LENGTH'}\n";
                        print TMP "Content Type: $ENV{'CONTENT_TYPE'}\n";
                        print TMP "Path Info: $ENV{'PATH_INFO'}\n";
                        print TMP "Translated Path: $ENV{'PATH_TRANSLATED'}\n";
                        print TMP "\n\n";
                        print TMP "\nSERVER INFO\n----------------\n";
                        print TMP "Server Name: $ENV{'SERVER_NAME'}\n";
                        print TMP "Computer Name: $ENV{'COMPUTERNAME'}\n";
                        print TMP "Gateway Interface: $ENV{'GATEWAY_INTERFACE'}\n";
                        print TMP "Server Software: $ENV{'SERVER_SOFTWARE'}\n";
                        print TMP "System Drive: $ENV{'SYSTEMDRIVE'}\n";
                        print TMP "System Root: $ENV{'SYSTEMROOT'}\n";
                        print TMP "Windows Directory: $ENV{'WINDIR'}\n";
                        print TMP "User Profile: $ENV{'USERPROFILE'}\n";
                        print TMP "Path: $ENV{'PATH'}\n";
                        print TMP "\n\n";

                        close TMP;

            }
}
```

Traversing the Corporate Firewall

by superbeast

Remember the day you started your new job at that major corporation? Finally, job security! Of course, your joy was quickly curtailed when you realized your only access to the Internet was via HTTP or HTTPS. No personal mail, no news groups, irc, vpn, etc., etc., etc.

What fun is a corporate job if you can't exploit it for personal use?

I needed my newsgroup fix and Google Groups was not going to satisfy it.

Discover

I did some researching and found a way to traverse the firewall using SSH. Now, SSH by itself is basically just a secure Telnet. However, many SSH clients allow you to perform Port Forwarding. Port Forwarding allows you to specify forwarding from a port on your local machine to a port on any remote machine via the SSH client. This means if you have a server at home with high speed Internet access, you can connect to it via SSH and forward ports through it. Then you can point your mail client or news client or any other client to the local-host:port and connect to the remote machine. People are currently using HTTP tunneling, but this is a way to tunnel any TCP/IP connection, and to work through your own or a friend's server.

Implement

I know what you're thinking - SSH runs on port 22 and the firewall has that blocked. Big deal! You have two options:

1. Via SOCKS

This method requires you to set up a SOCKS proxy on your server. You can configure the SOCKS proxy to listen on port 443 rather than the standard 1080. You can then configure your SSH client to use your SOCKS proxy server on the given port. This way you can send your SSH traffic through the SOCKS proxy and to port 22 on the local server. It can be referenced by internal name or internal IP address. Here is how I set mine up:

Home server
Name: gonzo
Internal IP: 192.168.1.1
External IP: 123.123.123.1
Configure SOCKS proxy to listen on 123.123.123.1:443. Configure SSH to use socks://123.123.123.1:443 as proxy. Configure SSH remote host as gonzo or 192.168.1.1.

Pros

You are obscuring the fact that you are running an SSH server by blocking port 22 and using SOCKS to connect to it. If you are scanned, most people will assume SSL and leave you alone. You also have a SOCKS server to use as a proxy for other programs if you like.

Cons

If you leave your SOCKS proxy open, others may find it and use it. The best thing to do would be to configure it to only allow connections to the local box.

2. Via port 443

This method is very similar: just set the SSH server to listen on 443 and set your SSH client to use 443 instead of 22.

Pros

Easy to set up.

Cons

If someone scans you, they may realize you are running SSH and try to connect or exploit it.

Conclusion

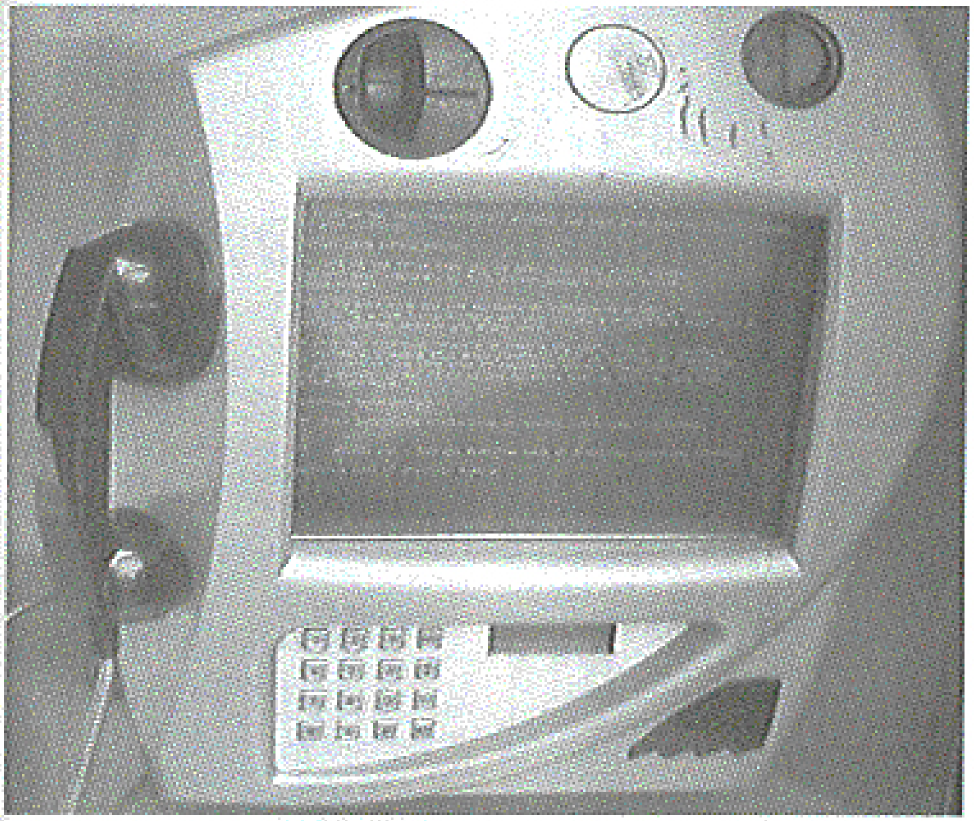
Once you get this up and running, you will see the power of using port forwarding. Not only can you use it for POP3, SMTP, NNTP, etc., but you can also use it for terminal services. Imagine opening an RDP client on your machine at work and connecting to your desktop at home! And to top it off, all traffic running through the tunnel is encrypted. If your corporate security group is sniffing or gathering traffic stats on you, none of this will show up. It will look simply like an encrypted session with your server.

Good luck!

Software Used

(these are all for Windows, but there are definitely Linux equivalents)

SSH Clients
SecureCRT - www.vandyke.com
SSH Secure Shell - www.ssh.com
SSH Servers (Windows)
VShell - www.vandyke.com
SOCKS 5 Proxy (Windows)
Wingate - www.wingate.com



These days you see the Blue Screen of Death everywhere. Here it is on an Internet payphone in London!

Photo by Glen Barnes

Staying Anonymous IN THE INFORMATION AGE

by Lucky225

Identity theft is a growing crime. Many people do not realize just how easy it is to obtain information and use it. Personal information such as your name, phone number, and address can be obtained as easily as making a phone call to a utility company such as your local electric or phone company. In this article I will run by a few social engineers I have used in the past that have proven to be reliable time and time again. I will also provide some solutions to help protect your information.

Scenario 1: Have name and address but need phone number.

A simple call to the electric company is usually all that is needed. The following pretext will show how easy it is to obtain an unlisted phone number.

Electric Company Representative: Thank you for calling Edison Electric Company. How may I help you?

You: Yeah, I'd like to check my account balance.

Electric Company Representative: Okay, what's your service address?

You: 2600 Hertz Ave. Beverly Hills 90210.

Electric Company Representative: Okay, I show a current balance of $92.68.

You: Thank you, and could you verify the phone number on my account. I tried entering mine at the automated prompt and it said it was invalid.

Electric Company Representative: The one we have on the account is 555-1212.

You: Thanks.

Scenario 2: Resident has recently changed their phone number.

A lot of people who like to keep their phone number private believe that if someone they don't want having their phone number somehow obtains it, that they will be safe by simply calling the phone company and having their number changed. A simple and easy social engineer proves otherwise.

Telco Rep: Thank you for calling Bell. How can I help you?

You: Hi, I recently changed my phone number, and the problem is I lost the paper that I wrote the new number down on. I feel so stupid.

Telco Rep: Oh, that's okay, what was the old phone number?

You: 555-1212.

Telco Rep: Okay, and you are?

You: John Smith.

Telco Rep: Okay, your new number is 555-1313.

You: Thank you so much.

Scenario 3: Have phone number but need address.

Reversing phone number to address is probably the easiest out of all the scenarios. An easy way to do it is to call a number such as 888-735-2872. This automated number is supposed to send you free information about Florida in case you are planning a trip there. They ask for your phone number and when you enter it it will read back a name and address associated with the number and ask if the information is correct. How can they do this? They get their information from magazine subscriptions and companies that sell such information. Another good way of reversing phone numbers to addresses is to call pizza delivery companies like Pizza Hut. A lot of the time these companies use your phone number to pull up your address quickly. All you have to do is call Pizza Hut and tell them you want a delivery. They'll then ask for your phone number and after you give it to them, they'll say, "And you still live at 2600 Hertz Ave.?"

And here's yet another social engineer involving a popular utility company:

Telco Rep: Thank you for calling Bell. How can I help you?

You: I'd like to check my balance.

Telco Rep: Okay, what's your phone number?

You: 555-1313.

Telco Rep: I show a current balance of $56.78.

You: Okay, my bill hasn't shown up in the mail yet. Can I verify it's going to the right address?

Telco Rep: I show 2600 Hertz Ave.

You: Thanks.

A lot of the time people use PO boxes for their billing address, but you'd be surprised how many representatives will give you the real address if you simply ask them to verify the service address on the account - the service address being the address where the phone service is.

Scenario 4: Obtaining Social Security Number information.

This is probably one of the harder social engineers to actually pull off due to the sensitivity of the information. However, I have been able to do it using the following social engineer. You will probably need name, address, phone number, date of birth, and possibly more information on the account. I've successfully obtained SSN information without much verification. The good thing about this is you can try it on almost *any* utility company.

Utility Company: Thank you for calling. How can I help you?

You: Hi. I'm trying to sign up for online billing so I can check my account through the Internet.

Utility Company: Okay, how can I help?

You: Well, I went to your website and every time I try to sign up it keeps telling me "invalid social security number." I was wondering if you could help me out.

Utility Company: Sure, what's your user name/address/phone number (depending on what utility you called)?

You: (insert information here)

Utility Company: Okay, the social security number I have on file is 000-00-0000. Is that yours?

You: Yes, I guess the website is just messed up or something. I'll try later, thanks.

Okay, now that I've shown just how easy it is to obtain information over the telephone, I'm going to give some tips to help protect your information. First of all, in the state of California, a utility company cannot deny you service simply for refusing to give your social security number. However, another form of ID such as a driver's license may be requested. Cellular companies are exempt because there has been no legislation restricting them. But the California PUC has this to say:

There is no requirement... that requires one to disclose his or her social security number as a condition precedent to obtaining telephone service. While a social security number may be requested as a form of identification, there is no requirement for a consumer to accede to that request... In retrospect, it is apparent that SB Cellular could have easily verified complainant's creditworthiness by other methods, such as by address, dates, and places of employment, mother's maiden name, or a host of other means less invasive of privacy concerns. In the future, SB Cellular is advised to take great pains to train its agents and staff to avoid a repetition of this type of incident.

If you are more concerned with people having your phone number more than your address, get yourself a pager or a voicemail box and give that out to anyone who you don't trust with your phone number. If you are concerned about your address information, you should have all your bills going to a PO box or private mailbox. The only thing left is your service address which remains your real address. You should put a password on all of your utility accounts. Never give pizza places your real phone number or name if delivering, or simply don't have things delivered to your house. Don't subscribe to anything and have it come directly to your house. Use your PO bOX or PMB as if it were your address. If you are concerned that giving out your phone number may result in the phone company giving out your service address information, you can use a cell phone and have the bill going to a PO box, or simply have prepaid cellphone service. If you have broadband Internet, you can sign up for voice over IP phone service at www.vonage.com.

Hardware Key Logging

by XlogicX
drkhypnos314@hotmail.com

A key logger is a device or piece of software or hardware that intercepts and stores strokes of a keyboard. I'll be focusing on the hardware key loggers. Hardware key loggers do have their disadvantages, though. I feel the benefits definitely outweigh the weaknesses. There are a couple of hardware key loggers out in the market. I'll discuss one of the more popular ones. I'll also go over the theory of how they work and how one could be built (if you're afraid of being "secured" by the "homeland").

Disadvantages of Hardware Key Logging

Limited Storage: The storage space is one of the first notable limits. With software key logging, the limit is usually the size of the free disk space on the hard drive. The limit of the commercial logger I'll go over is only 64K. It may sound bad in comparison to all of the huge hard drives out there, but if you think about how much text is required to take up 64K, it's plenty enough to get accounts and passwords. Also, if you make your own logger, the limit is however much EEPROM (Electrically Erasable Programmable Read Only Memory) you wish to purchase and are able to address.

Visible Detection: If the back of the computer is visible, the logger is pretty simple to see. It looks like an inch long PS/2 adapter. Though it doesn't look suspicious, it is still visible. One thing I would do to overcome this disadvantage is get a PS/2 extender cable and connect the logger below the computer somewhere out of site.

No Control Characters: The commercial key logger can only record alphanumeric keys, spaces, and backspace. It's understandable by the way it operates, which I'll go over later. One way to overcome this problem is to just build your own logger.

Requires Physical Access: Yes, you do need to physically access the computer. This is probably the biggest disadvantage. The only thing that I can think of to help around this one is to pick up the hobby of lock picking. Though, it is surprising how many important computers can be left unattended and physically accessible.

Benefits of Hardware Key Logging

BIOS Password: The hardware logger starts operating as long as the keyboard gets power, so the BIOS password can be logged.

OS Independent: Since the logger operates independently from software, it doesn't need to interface with an OS to log keys. Accessing the log is slightly different, but not terrible.

Undetectable with OS/Software: The logger is hardware, it doesn't suck resources, doesn't appear in task list, or on hard drive. It also doesn't cause any noticeable lag from keyboard to computer.

Login Access Not Required: There is no need to log in or start the computer to install the logger. There's also no need to send any software as an attachment. All that's necessary to get the logger up and running is to plug it into the back of the computer.

KeyKatcher

This is the commercial hardware key logger that I'm most familiar with. I purchased it at www.keykatcher.com for about $80. That price is pretty steep, but depending on what you do with it, it can be a valuable tool for your privacy. I have mine connected to my computer just to see if my roommates are snooping around on it. This device looks like a small PS/2 adapter. It is connected in between the computer and keyboard chord. The software recommended to access the logger is Notepad (although you can use anything that contains a text field). You open up Notepad and type the default password (keykatch), and a display like this shows up.

```
keykatcher 64K 3.7
065518 bytes free
1-View Memory
2-Erase Memory
3-Change Password
4-Disable Recording
5-NETPatrol Output
6-Search for String
7-Exit
```

View memory: Dumps everything on the logger into the text field of Notepad. It is slow (could take an hour if full), but can be worth the wait.

Erase Memory: Does exactly that, takes about 15-20 seconds consistently no matter how full the logger is.

Change Password: Allows you to change password, can't be more than eight characters (shame), and has to start with an alpha. A tip is to make the password something that you wouldn't normally type, especially one of your normal passwords. The reason for this is that right when you type in your password for your email, the keykatcher prompt will come up in the password text field, not too fun.

Disable Recording: Effectively makes the key logger nothing more than an extended wire chord.

NETPatrol Output: Finds all www, .com, .nets and displays what surrounds them.

Search for String: Allows you to enter your own string and have it searched.

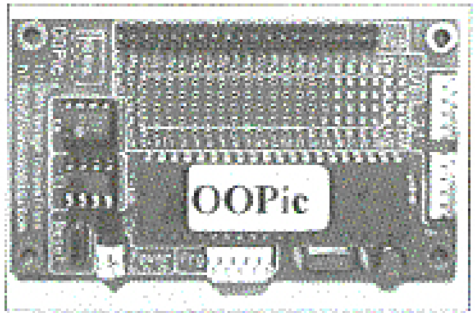
Exit: Gets out of prompt. Any other input other than 1-6 will exit too. Exiting can be more important than you think. If you just close Notepad and go into something else and accidentally type the number 1 (or the other five numbers), it will reset to it.

How It Works

This is basically a big buffer with some firmware. You type a character over your keyboard, it goes to the logger, stores it, and passes the same info through to the computer. It can't store all keystrokes because some of them are treated as executable commands. It displays the backspace as "//". The reason for this is that if it tried to display the backspace, it would execute it instead and you wouldn't see it, along with enter, control/alt/delete, and many other commands that aren't even on your keyboard. That's what gives you the ability to use text-editing software, since the logger itself can send low-level commands to the computer. So it isn't just limited to Notepad or Word. I've used it on emacs and AbiWord as well.

Some Theory for Building a Logger

This is definitely more work than it's worth to most people, but that's what hackers are for, right? I would start with some small and easy to use microcontroller. There are many to choose from (68HC11, Basic Stamp, OOPic). I would choose the OOPic (Object Oriented Programmable Integrated Circuit).



The OOPic is relatively small, can store 64K of EEPROM, and can be programmed in Basic, C++, or Java. I use C++ just out of familiarity. I purchased this from a distributor I found from www.oopic.com. The development kit set me back $70. The benefit I like with the controller is all of the objects that are included with it. The most relevant object for this application would be oSerial for obvious reasons. You can set the baud rate and everything. From that point on, connect the wires from the keyboard's PS/2 connector to some defined input pins on the OOPic, then wire some output pins up to a PS/2 extender, and connect the extender to the computer. This will probably require some soldering, unless you've thought of something creative. For the programming, write a program to store the incoming serial keystrokes as a list, and then send those strokes out to the computer. The fun part is figuring out what data means what stroke. That's one of the fun parts of hacking; you poke around at something, look at the data, try and figure it out, and learn more about how the technology works.

Ethics

If you use the commercial logger as your sole tool for getting into systems, you're at the level of script kiddie. Building your own is recommended, since it may force you to learn a little. I have gained access to others people's computers this way, but I tell them that I did it afterwards. I tell them how I did it too, and I still even feel a little dirty. Then again, they are more secure with the knowledge of what's out there, and probably won't let it happen again (cause they look around the back of their computers by routine now).

Shouts: Medicine Soup and James.

Peeling Grapes

by Bryan Elliott

There are many reasons to want to rip the archives of a website. Most of them involve instant and offline access to cool stuff with no advertisements.

The important thing to remember here is that you want to peel the site, not rip it. The distinction here is simple - *peel* the website and you allow other people to use it, and usually don't end up making their ISP have a conniption. *Rip* the website and you've cost the makers of stuff you like a good deal. You may have also cost them advertisements; when you're utilizing all your bandwidth to tear at theirs, you may keep others out.

So, as a precaution, remember to keep the bandwidth controls on your software. I mean, you don't want your favorite public domain MP3 site going down when you suddenly pull ten gigs (a lot of money in bandwidth terms) worth of stuff in a little over a day, right?

Watch Your Language

I've been criticized for loving PHP. People tell me it's not a real language, it's for pussies, and such. All I have to say to them is, piss off. PHP is well designed for what it is: a brilliantly souped up data processing language. It's got simple interfaces for network connectivity, file access, Win32 API functionality, the wonderful PCRE libs, and it makes quick and dirty development a joy. If you think I'm a puss for that, then I can only say "Meo-oww, baby."

What Would We Peel?

Say, for example, you're a comic connoisseur. *Megatokyo*, an excellent webcomic, has their comics serially numbered, from zero to whatever comic is currently listed on the home page. That's a simple chore to write code for. The pseudocode goes something like this:

```
Open www.megatokyo.com, port 80, send "GET /
    HTTP/1.0<crlf><crlf>" (standard
      dumb browser request)
Parse out today's comic image name
figure out how many we must get to be up-to-
    date from previous attempts
for last_saved+1 to current:
 open connection
 send HTTP header
 check response for error
 if response = 200, save the image
```

See? Easy.

Why's This Grape Shaped Like A Stapler?

Well, it's not always easy.

See, *Megatokyo* is a bit of an exception in comic bookkeeping. *Penny Arcade*, for example, works on a date and scripting system. What method are we to use to get around this?

Quite literally a different method indeed. We still count past all the possible dates, but instead of using GET, we use the HEAD http method. For example, a good "idiot light" for a webserver is to telnet to port 80 and type in "HEAD / HTTP/1.0". If you get 200, you're OK.

So, the new pseudocode is:

```
Get today's date.
Store November 18, 1998 somewhere. Since this
    is Penny Arcade, your use would be an
        appropriate spot.
Check to see if we have already got some penny
    arcade. If so, get the most recent date we've
        downloaded, add one, and replace Nov 18,
            '98 with it.
For last_date to today:
 send HEAD request (keep connection alive;
     might as well with all we'll be doing here)
 if response is 200, send an equivalent GET request
 save the image
```

Right. Just so's you know, it's going to be a little different each time you do it. I'm just trying to teach you the necessary skills for website peeling.

New Tasks, Closing Arguments

Now, sometimes you'll have to have your program selectively pick images from a webpage, choosing content, but avoiding stupid things, like adverts and buttons. This is where PCRE matching comes in.

For example, the Page3.com, softcore porn it is, is a fun page to try ripping. Twenty some girls, an average of 60 some pics of each girl. And, being the manly hacker-type you are, you must have every image. All of 'em.

So? As said, you can make use of PCRE, or Perl-Compatible Regular Expressions. In PHP, it's built in, and in C/C++, there are libs and DLLs for you to use, and in Perl... well, they're called perl compatible for a reason, ya? Use whatever you prefer.

I was going to post up the code for this process, but quite frankly, I'm at work, and pulling up softcore porn, while fun to do at home, is not the smartest thing to risk having your coworkers see. As such, I'll let you do the research and exercise yourselves. I'll leave you with links to the relevant documentation.

http://www.php.net/ - PHP: a nice handy language for the starting programmer.

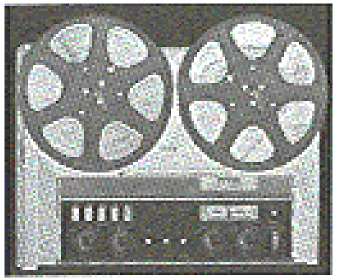
http://www.cs.virginia.edu/~lcc-win32/ - lcc-win32: a lovely ANSI C Compiler for windows programming.

http://www.pcre.org/ - PCRE: the dlls and documentation, and everything you need to know about PCRE. You must welcome the headache.

Just a quick note on PHP: If you want to try it out, get the 5MB package. You can't play with all the cool functions without it. Additionally, an easy way to find stuff is to simply put your search terms after the initial slash. I'm serious here. http://www.php.net/preg_match will get you the docs for the preg_match() function.

Just remember to keep it down to one connection at a time, please.

Microphones, Laptops, and Supertaps



by Dark Spectrum

PC microphones are everywhere. They're in the home, the workplace, and in schools. You often see omni directional mics like the Labtec Verse 303 or AM-232 mounted high up on computer monitors. You're careful what you say near them since you know how good their room pickup is and how easy it is to capture the audio stream from a PC mic. After reading this article, you'll watch what you say near *any* mic.

The PC might have a benign or even trustworthy owner, but how can you be certain it hasn't been compromised by a third-party eavesdropper? If you think about it, the idea of a hijacked mic is frightening. It's much more effective than a wiretap - it can be set up from thousands of miles away and uses existing, innocuous-looking equipment to create a 24/7 monitor on an entire room or office cube. Call it a "supertap."

When you see a lab, office, or school room full of PC's with omni mics, it's time to think back to Heinlein's classic *The Moon is a Harsh Mistress*. The only difference is that the PC mics are loosely connected via a network of systems rather than directly to a single computer. What could anyone possibly do with such an overwhelming stream of information? Lots of things: simple old VOX (voice operated transmission) or the newer VAD (voice activity detection) techniques can reduce the bandwidth a lot. Specific speakers or topics can be picked out via speaker recognition and speech recognition technologies. Simple correlation-based methods can track a specific individual through a field of microphones.

OK, so much for omni mics. But what about the others? (And there are *lots* of them.) Directional monitor-mount mics like the Labtec Verse 313/AM-240 or the directional desktop boom mics? Close-talking mics used in those PC headsets you see lying on desks or hanging from cube partitions? Don't forget that almost every laptop has a tiny built-in mic which is exposed when the laptop is open. But what if the laptop is closed and buried in a docking station, or left disconnected and lifeless on a conference room table?

The chilling truth is that any of the above configurations makes a perfectly good bug for the PC's immediate vicinity, and some of them are effective enough to form the basis of a supertap. It doesn't take any rocket science, either. All that's necessary is to use 16-bit audio and adjust all recording gains to their maximum values.

The only black magic is in the dynamic range provided by 16-bit audio. Most PC audio systems lose three or four bits to noise, but that still leaves you with at least 12 usable bits. You can record an almost-inaudible -48 dB signal (0.4 percent of full scale), boost it by 256 to normalize it, and still have four bits or 24 dB of signal available. The high gain will create highly amplified noise, and the four-bit speech won't sound good, but it will certainly be intelligible.

Don't believe me? Then why not just try it to see what you pick up. It's easy. Use the Recording Control panel (sndvol32.exe) to make sure the mic is selected, and to set its gain to max. If you have a laptop then it might have a dual-purpose line-in/mic jack and in that case you should click on the "Advanced" button to verify that the microphone boost is enabled. Use your favorite audio editor for recording. If you don't have one, then you could use the basic Windows recorder (sndrec32.exe) but two much better choices are Cool Edit (www.syntrillium.com) and Gold Wave (www.goldwave.com). Whatever editor/recorder you're using, configure it to 16-bit mono audio in linear PCM format. Your system might be able to get good recordings at 8 kHz but for now just play it safe and set the sample rate to 11.025 kHz or 16 kHz.

You need good audio output to hear the results. Headphones are best, but external speakers are also good. You will probably have to boost the output level. That can be done via your headphone/speaker volume controls and system playback gain controls (sndvol32.exe again) but you'll get less distortion if instead you use Cool Edit or Gold Wave to normalize the audio before playing it back.

There are two microphone configurations that are particularly challenging: high-quality PC headsets and docked laptops.

Cheap headsets are no problem. They pick up any sound, from any angle, in any position. High-quality headsets with close-talking mics don't. For example, the Andrea Electronics NC-65 stereo gamers' headset with anti-noise features seems to live up to its claims. Even so, it records ordinary speech five feet away as -48 dB and as already calculated that's all it takes. The background noise is steady (wide-sense stationary to you DSP types) which means it's easy to develop a custom speech detector for it. Chalk up any PC headset as... supertap-capable. For a long-term test you'll need to record to disk and use a speech detector. Those features are found in utilities developed by scanner/ham radio hobbyists, examples being Scanrec (www.davee.com/scanrec/index.html), Vox Recorder (freeweb.supereva.it/radio/VoxRecorder/index.htm), and RecAll (www.sagebrush.com/recall.htm).

Docked laptops don't work as well. There are two reasons for that. First of all, high frequencies are attenuated by the narrow passages the sound has to pass through to reach the mic. That makes consonants harder to understand, masks some of the cues people use to recognize speakers, and reduces faraway speech to meaningless mumbles. The second problem is that the mic might have lots of noisy neighbors in there: fans and disk drives. Fans produce continuous noise due to air flow. Disks emit transient clicks that are hard to filter out since they aren't a steady noise; if you're experimenting with a built-in laptop mic then *don't* log the audio to disk. For a worst-case scenario consider the (aging) Dell J650: its docking station is fully enclosed on three sides and the mic is centered above the keyboard far away from any open air, but it can still pick up speech from the immediate vicinity. Newer Dell laptops use open-frame docking stations with the mic on the right side of the keyboard so it's much closer to free air and therefore produces better recordings.

I'll close off by explaining the "disconnected and lifeless laptop." Modern laptops have power-management features which allow you to configure how they behave when the case is shut. It's sometimes possible to configure them to simply keep on running when closed up. That still leaves those blinking LED's, but any doofus with a screwdriver and wire cutters can disable them. What's left is a high-capacity, highly configurable data logger. It isn't likely to be hijacked by a third party, but it's still worth mentioning as a mic to be wary of.

OPTIMUM Online and You

by Screamer Chaotix
screamer@hackermind.net

For years the telephone companies of the world have pulled the wool over their customers' eyes, forcing ridiculous charges upon them and blinding them from the truth. Hackers rose against this, pointing out these injustices and showing everyone exactly what was happening with the technologies they knew nothing about. Now, a new threat is present. Only this time it's not the telcos, it's the cable companies.

This article will focus on Optimum Online, a well known cable modem provider in the Connecticut/Long Island area, but I'm certain these tactics are in place all over the country. Optimum Online, like other cable providers, sells you a cable modem and NIC through The Wiz retail outlet, along with their service. Upon installation of their hardware, you register with them online, where you are then presented with their terms of service (mind you, you've already purchased the equipment). Once set up, you're ready to go and, like most people, you'll be amazed by the high speeds.

However, if you're like me, you had a few questions before you made your purchase. The first, in my case, was a simple one: "Is this equipment compatible with Linux?" The man at The Wiz assured me it was, although Optimum did not support that particular operating system. I looked at the NIC and noticed it was an ISA, which didn't sit well with me. I asked for a PCI, but he said that's the only one they had. Fair enough. I had his assurance it would work with Linux, so what was there to fear?

That was the first problem, but it certainly wasn't the last. The NIC did not work with Linux, and the only way it would was if you wrote your own driver more or less. Unfortunately I really didn't have that kind of time, especially when I was told it would work out of the box. Nonetheless, time went on and I eventually got a card that did work. Problem solved. I was now online and enjoying the incredible speed of my cable modem. Here was where the new problems began to creep in, as pointed out by this email I received from Optimum themselves:

Dear Optimum Online Subscriber:

You may be running a server from your computer and not even know it.

If you use any of the peer-to-peer file services listed below without disabling the file sharing option, the entire Internet can access the files on your hard drive. In addition, use of these services can lead to network problems that may result in your upstream speed being temporarily reduced to control this abuse of service.

Aimster, KaZaA, iMesh, Audiogalaxy, eDonkey2000, NeoModus, BearShare, Gnotella, Gnucleus, GTK-Gnutella, LimeWire, Mactella, Morpheus, Phex, Qtella, Shareaza, SwapNut, XoLoX

Don't compromise your privacy or the performance of your high-speed connection.

First they "alert" me to the dangers of these file sharing services and then, one sentence later, say they're an abuse of service. Wonderful, now by merely using KaZaA I was violating their terms of service. How you ask? Running any kind of server on Optimum's network and, as I said, other cable networks most likely, is strictly prohibited. So running KaZaA is a violation of my terms of service, and should I continue doing it, I may be punished. A part of me wonders if the RIAA or MPAA are standing in the shadows, but I won't go into a conspiracy theory.

There's a problem here. The terms of service basically give the cable company the right to declare anything a server! Next week ICQ might be forbidden, using DCC could be outlawed, and forget about running telnet, ssh, or ftp on your computer. They claim servers pose a security threat, yet I don't understand why they won't let me take my own chances. There are people in this world who use the Internet for more than just email and web browsing after all.

Which brings me to my next point - websites. By now it should be no surprise that many cable companies oppose running webservers on their networks. Out of curiosity, I found myself playing around with Apache one day, just to see what would happen if I set up a site. I made up some html files, threw them in /var/www/html, and went to my IP via my 192.168 address. There was my site, clear as day. Next, I opened port 80 on my layer two switch and asked a friend to head to my IP using a web browser. He did, but could not see anything. All right, they were filtering port 80. I changed around httpd.conf so that both "Port:" and "Listen:" were set to 81 and asked him to connect again. This time, it worked.

This however, did not last long. Today it does not matter which port I use. All incoming http requests are filtered at the gateway. What does this mean? It means I can run a webserver on any port I like and then telnet to the server:port to see that it's there, but making any sort of http (or https) request leads to a connection timeout. Great, now none of my friends can see my site.

My solution was really quite simple, although far from practical. I merely installed VNC (Virtual Network Computing) on one of my local machines and gave the IP/port to my friends. This allows them to connect to my internal machine through VNC, open a browser, and see my site as though they were on my LAN. Of course, it's sad I have to take such measures. All I want to do is use the Internet the way it's meant to be used. Why must there be so many restrictions? You pay for your allotted bandwidth and, as long as you don't uncap your modem, you should be allowed to do whatever you wish.

I'm certain there are people who disagree with what I've said. Many have told me the terms of service are what they are, and if I don't like it I should go elsewhere. I'm not really sure where I can go... DSL I suppose, but why should I have to go through the hassle? There are a number of other things I could rant about, but I think what I've said is sufficient. We mustn't let these types of things continue. If we do, one day we'll find ourselves paying for every download, or getting booted because we had the nerve to run ssh. Unless we stand up against the ISPs, we may never have true, unfiltered Internet access.

Shouts to Dash Interrupt, Panther, Leland D. Peng, Sparky, and Jack Bauer.

CYBER Cafe Software Security

by minion

Cyber cafes are popping up all over the world. The purpose of cyber cafe software is to restrict the user depending on purchases and security purposes. In normal cyber cafes there is usually one server running the server software responsible for managing and serving customers, and the rest run the client software which contacts the server for information like user/password info, item purchasing, time purchasing, etc. You would think that security would be a huge priority when working directly with the purchase of time and direct money use. Ironically though, cyber cafe software can usually be bypassed with ease.

The piece of software being covered here is Tinasoft EasyCafe, claiming to be "The best Internet Cafe Management Software in the World." Bold statement, eh? EasyCafe works like this. On the server is the EasyCafe server software. It handles all EasyCafe connections, user details, socket info, accounts, prices, time distribution, balances, log files, transactions, even food orders! The admin on the server can also get continuous screenshots of any client, send popup messages, and some other features.

Now on to the fun stuff, the client software. Careful when testing cafe software. It is extremely easy to lock yourself out of your own computer! There are three files which play a role in EasyCafe's security.

Client.exe - client application. Handles server requests, time, orders, billing info, etc.

Guardit.exe - monitors escape keys (not very well), task manager, and other potentially dangerous things.

Easy.cfg - configuration file for Client.exe

Client.exe doesn't have much fun stuff in it but Guardit.exe and Easy.cfg sure do. Guardit.exe keeps you from simply being able to alt+f4 the main login screen. Well, what happens when it can't be started? The program freaks out and closes itself and tells you to contact the system admin!

So how exactly do you get this to happen? It's simple. Just rename Guardit.exe to anything else and then kill the Guardit process. Killing the process could be a pain if you're trying to use Task Manager, considering that running Guardit closes Task Manager every time you open it, so let's just use cmd.exe.

```
C:> rename "C:\Program Files\TinaSoft\Easy
    Cafe Client\Guardit.exe" Guardit.bak
C:> tskill Guardit
```

Wait a couple of seconds after you type this and you should be prompted with an "OK" box saying "ERROR:: GUARDIT.EXE CAN NOT BE STARTED..! PLEASE CONTACT YOUR SYSTEM ADMINISTRATOR." After hitting OK you will be returned to a computer free of the restrictions placed by the server and client software.

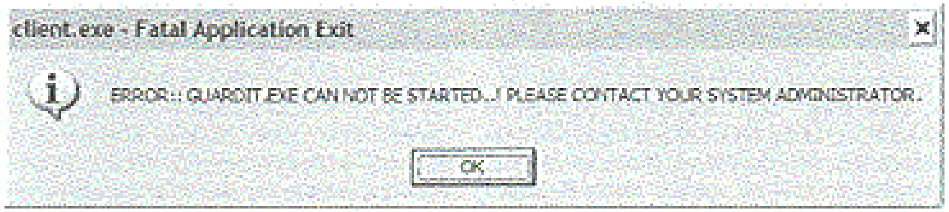
It gets easier though. Guardit.exe is based on time intervals. If you hit ctrl+alt+del and Task Manager pops up, it takes a couple of seconds for Guardit to close it. Can you see the flaw yet? Guardit is also what is responsible for making sure the client isn't closed. Quickly killing Client and then Guardit immediately after will also return you to an unrestricted computer!

```
C:> tskill Client
C:> tskill Guardit
```

Believe it or not, there's more. The configuration file has come back to haunt EasyCafe. The configuration file is where the server's IP address is stored. Simply changing the server's IP to another that's pre set up with unlimited time will obviously bypass what the software had intended. The file should look something like:

```
   127.0.0.1      "ŕΩø6$¥/®x"¯-¿
P3˜ž•Ï Ì2≥'ÛáÇ9Ü‹Ïÿÿ(Ì<™ïàe/S‹±±H"
 Δ4 6</ R?-J ∏z'#‹          ÁuŸÔ«C ÁO`?"
  ÛõQ1ê% '_2&-ïj-ü" "ä? â 52á T3/öYÂ
   ¬D»"Σ"°°2i
```

The first parameter, 127.0.0.1, is the server IP address. A quick change in the configuration and you're done.



client.exe - Fatal Application Exit

ERROR:: GUARDIT.EXE CAN NOT BE STARTED..! PLEASE CONTACT YOUR SYSTEM ADMINISTRATOR.

A Coupon Trick

5 2 1 0 0 0 2 7 5 7 5 0

by Charles

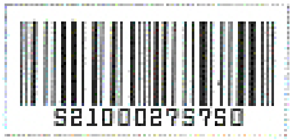
A manufacturer's coupon for 30 cents off Philadelphia Cream Cheese was found inside the lid of a prior purchase. The UPC code was very short and there were repetitive numbers in the second half of the code. Knowing that the first portion is the manufacturer's ID number and the second half being "23030," I wondered if the "3030" was the face value of the coupon repeated. (The original coupon UPC code was: 5-21000-23030-8.)

Knowing the last digit (8) is the checksum, I popped over to http://www.barcodesinc.com/generator/barcode/ and typed in: 52100027575? (the question mark causes the CGI program that creates UPCs to determine the new checksum on its own).

Now, popping over to the Kraft web site - I got some graphics and quickly pasted them all together with some text in Photoshop (just to prevent any potential problems if someone saw the coupon - a black and white UPC on plain paper might get some attention!).

Now to put it to the test - could hacking this 30 cent coupon up to a 75 cent coupon be that easy? I went to a local store with a self-checkout and purchased one container of Philadelphia Cream Cheese (which was $1.99 and had 30 cents off (store sale)). Now the test. Scan the coupon. The worst that could happen is that the UPC would be "not on file," right?

Bingo! 75 cents off, plus 75 cents off (my store doubles manufacturer coupons!), plus 30 cents off (store sale). Total sale: 19 cents. Now I'm wondering about other coupons that use this short form of the UPC used with coupons.



Hacking the Look

by Rev. Karn - ZenLogic/Freebooter

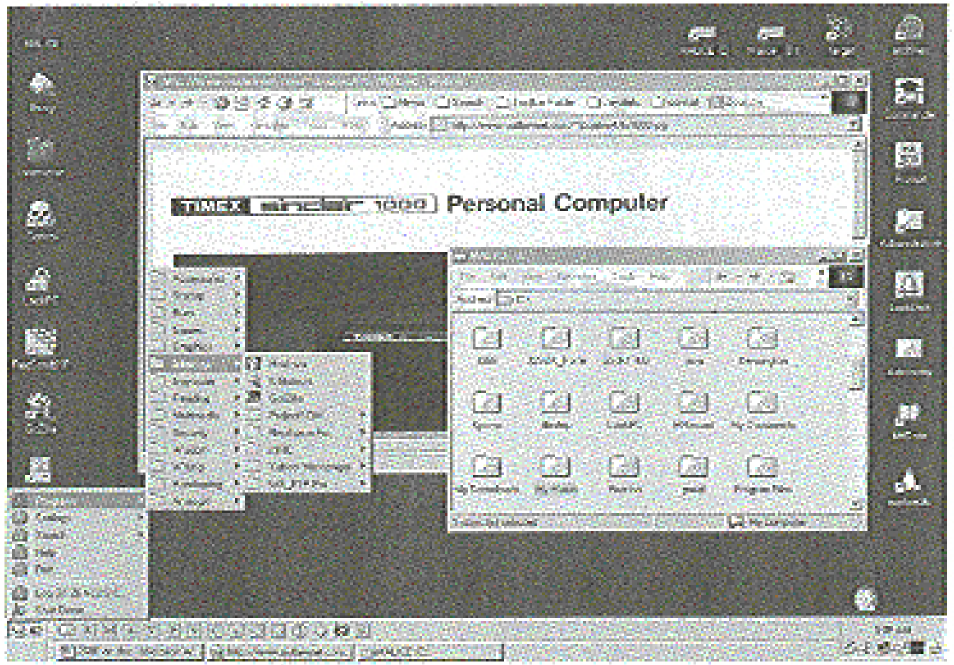
This is not an article about hacking the mainframe or some network someplace, but an article about something much closer to home. Your everyday Windows box. These visual hacks will work on most flavors of Windows. Have fun and read the caution below.

Caution: First off, doing these hacks can mess up your system. Remember to back up all important files, and that includes the registry. Make a copy of all the files that you res-hack, copy the dllcache to another directory just in case, and rename. Then empty out the old dllcache. Make a new up-to-date ERD disk and be careful. Let me say this again: *be careful.* The program I used the most was Res-Hacker (Resource Hacker 3.40 by Angus Johnson), a great little file for hacking system files and retrieving resources. (Google it.) Use the program a bit beforehand. You will find that it is self explanatory.

Background

I have been obsessed with computers for a long time now. In fact, my first computer was a Timex/Sinclair 1000. After that came the Tandy, then various Commodores, an old Osborne, an AT&T 6300, then over the years a bunch of 386's, 486's, and Pentiums. Now my systems consist of mostly (eight) home brew computers, a variety of CPU's from the low end of a 300 MHz over-clocked Pentium 2 to the high end of my brand spanking new Sony laptop - 1.5 MHz mobile Pentium 4. The rest are mostly AMD 700 and 850 MHz systems. All running a Mulligan's stew of OS's from Windows 3.1 to Linux (Free BSD and Mandrake - I have one old 286 laptop running Minux), and one Apple Performa running OS 7. A D-link DSL 4 port router and an SMC 8 port hub connects it all together. One box is a file server for the storage of overflow files. I have eight kids. Do you know how many Pokemon jpegs are out there? Yes, they have saved them all.

My first hack was setting the 6300 up with 9600 baud modem, a packet driver, and an early trumpet like program, then social engineering my way into a university's modem room phone number and getting on the Arpanet back in 1983 when it changed over from ncp to tcp/ip, so I could use usenet.



This article is about my laptop and the OS hacks I had to do to make it truly my own. Let me explain. The laptop, named mAlice (mobile-Alice, at least one of my computers are always named Alice, don't know why) is the work computer. The one I drag along to the job site with me. I am retired and administer several small business networks in the surrounding towns for extra income. Anyhow, malice boots into Elo. From there you can choose Win2k or Mandrake. Default is Win2k. Also on the Windows side I emulate Mac OS 7 using Basilisk (for compatibility with the kids' school files., boot to Mac, convert the files, drop them onto the NTFS partition, there you go. The kids can now work on the files at home.).

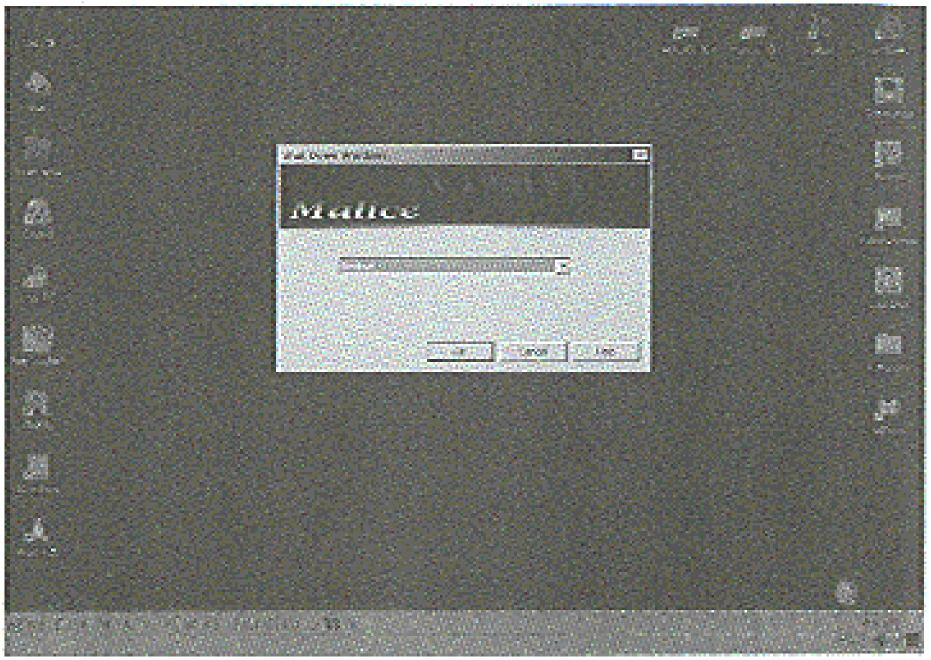
The Hack

As you know, Win2k looks horrible, so when I'd pull out the laptop and boot to Windows, it looked like all the other computers out there. Real embarrassing. I the great Zenlogic with a plain Jane machine... (way too much time on my hands now that I'm retired!) so I tried to do something about it. Out came Res-Hacker. I started looking at the system files in the OS and looking for the start button and other resources. I wanted it to look like a Linux box, so I starting hacking away at things. (Yes, I know there are programs out there to do this but I didn't think it would be that hard. How wrong I was and, yes, I have tried Black Box and KDE, on top of Cygwin. However I wanted to keep that part of Windows the same because I install and uninstall programs all the time and neither Black Box or KDE for Windows really works right in that regard.)

First, we need to turn off Windows file protection (an almost impossible thing to do). Microsoft's way of protecting us from ourselves and their answer to dll hell. I know that there was a registry hack to disable it.

(HKEY_LOCAL_MACHINE\SOFTWARE\
    Microsoft\Windows NT\Current Version
        Winlogon)
Value: *SFCDisable*
Type: *REG_DWORD (DWORD Value)*
Value: *0 = enabled (default), ffffff9d = disabled*

Thank you whoever you are at the "microsoft.public.windowsxp.general" newsgroup. However I quickly found out that this only works on Win2k pre SP3. Now, what do I do? I went back to the newsgroups. I found an obscure article on the overclockersclub.com website: "How to Disable the System File Checker in Windows XP" dated March 4, 2002. I tried it on Win2k and lo and behold it worked. Here are the main points.



Windows XP No Service Pack

Backup sfc_os.dll (sfc.dll in Windows 2000) in the \windows\system32 (winnt\system32 in Windows 2000) directory. Make another copy of sfc_os.dll (or sfc.dll), call it sfc_os1.dll (or sfc1.dll), and open with a hex editor. Go to offset 0000E2B8 (0E2B8h). You should see the values "8B" and "C6".

Windows XP Service Pack 1

At offset 0000E3BB (0E3BBh) you should find the values "8B" and "C6".

Don't do anything if you can't find these values. (When I looked in the sfc.dll file in Win2k the 8B C6 values were there.)

Change "8B C6" to read "90 90" and save.

Now on my computer I just rebooted into Linux and copied files, which solved the problem of replacing files in use, but the article on overclockers.com said this:

"Run these commands to update the system files:
Copy c:\windows\system32\sfc_os1.dll c:\windows\system32\sfc_OS.dll /y
Copy c:\windows\system32\sfc_os1.dll c:\windows\system32\dllcache\sfc_OS.dll /y"

I take this to mean boot with a boot disk or F8 to a command prompt and run the commands from there. OK, if all goes well, we just have a couple of things left. If you are asked for a CD ignore it. Remember to reboot and fix the registry like I did with the SFCDisable Reg hack. You must do both in Win2k to turn off file protection. Reboot, you're good to go. Check if it worked by going into the event viewer and looking for an entry like this.

```
Event Type:       Information
Event Source:     Windows File Protection
Event Category:   None
Event ID:         64032
Date:             4/16/2003
Time:             3:48:14 AM
User:             N/A
Computer:         MALICE
Description:      Windows File Protection is
                    not active on this system.
```

OK, now we can really start changing things. Remember, this is Windows, so things aren't where you would think they would be. Let's start with the boot screen background bitmap, use Res-Hacker to open Ntoskrnl.exe, look for bitmap #1. Replace the bitmap with one of your own choosing. It must be a bitmap file that is 640x480 with 16 colors. Or find one on the net, search for boot logos, or modify the one already there. Save, reboot, and admire your new boot logo. Next I wanted to change the Start button. But where did Microsoft keep the string table for it? Yep, explorer.exe. So I opened it up with Res-Hacker and there it was. String Table -37 -1033. On the right, you should see the word "Start". You can change this to anything you want, as long as you don't go over five characters. Now hit the Compile Script button. Go to String Table -38 -1033. Again, on the right you should see "Start". Change this to the same as the previous one. Hit the Compile Script button again. Now there is the little problem of the Microsoft icon on the Start button. That can be changed too. Res-Hack back to explorer.exe and look for bitmap -143 -1033. You can use a pre-made image or make your own. It must be a bitmap file 25x20 by 16 million colors. Save and reboot. But a problem cropped up after I hacked everything. I just couldn't save it. I left it in frustration for awhile, watched some dbz with the kids, and then it hit me. Duh, can't save because it was in use. So I used Task Manager to close Explorer and then alt-tabbed out of it to Res-Hacker. Saved, then rebooted. Cool, it worked! Now we are getting someplace. New boot logo and a Start button that has lost all traces of Microsoft. Good to go.

Next was the Microsoft bitmaps and logos appearing on the "starting" and "login" box while logging in, also when hitting "ctrl-alt-del". Where were these resources? I looked and looked and couldn't find anything. Then I remembered I had a problem booting not too long ago and the log file from the event mentioned msgina.dll. So I opened it up and there they were. I pulled these resources to find out what size bitmaps they needed to be. They had to be a width and height of 413x72 and 16 bit bitmap. I converted the bitmaps I had picked out to the size needed and replaced the old bitmaps. Saved and rebooted. Cool, but things were still Microsoft blue, back to Res-Hack. Saved out the bitmaps and such, changed colors and replaced them, saved and rebooted. Good to go. Now malice looked good. Except for one thing, the logon applet. Still the Microsoft blue and no graphics or such. I was stumped! How the hell do I change that? I could change the color of the start screen with a Reg hack. Black of course.

(HKEY_USERS\DEFAULT\ControlPanel\Colors\\Background change to FFFFFF)

But the logon stayed the same. Well hell. Took a few days to think about it, meanwhile searching on Google. Not much help, but ran across a freeware program called "Crash Course Logon Interface" at www.crashcoursesoftware.com. Turned out to be just the thing I needed. Check it out. That taken care of, there were all kinds of icons and bitmaps in the various dll and exe files in Windows and to change them all would take forever. So here is where I cheated again and used a program. One day on Google I ran across a Japanese software site. I found what looked like a program for changing the icons in Windows. I downloaded it, and sure enough it was. Here is info on this very nice program:

Masami Ikawa
Madonote ver6.01 for Windows
Filename WHAND601.EXE
http://www.asahi-net.or.jp/~vr4m-ikw/Global/download.html

A nice program for sure. It made my quest a lot easier. Try it. I changed almost all the icons in my system. The ones Madonote didn't do I Res-Hacked. Now we have a pretty visually different desktop. There are other things I didn't like about Windows. The plain menu bars, etc. Using Res-Hacker I opened explorer.exe and other such files and dll's, did some changing here and there, had all kinds of fun, messed up a few times, put it all back, and started over. "So it goes." Now I have Win2k looking just right for me. A friend dropped by one day, saw the desktop, and thought I was in Linux with a new theme. It was great.

It sounds easy now writing this, but at the time it really sucked. I even screwed the registry up a few times and lost Windows. Thank God for backups. All in all, it took me several days of work, thinking, and searching the newsgroup archives to redo the look of malice. Finally, after much frustration and a few episodes of dbz (from fat bu to kid bu), in the end it all worked, and malice looks great. That is why I decided to write this, to put this information in one place. Now when the rubes look at my box top, they are always asking what OS I use and the women, well, that's another story. Now if I can just make the lilo boot-splash look different....

Thanks to all the people who have posted replies to the newsgroups in the past (newsgroups are a great resource for any kind of information). I tried to find the old posts, quote them, and give credit. However, most are gone now or I could not remember where they were or find them again. Sorry if I missed somebody. You know who you are. Thanks.

By the way, howdy Joe (Joeschmoe).

HOSTING AN FTP SERVER

on Cable/DSL Routers

by osiris188
Updates81@hotmail.com

In 19:3 Khoder Bin Hakkin wrote a great article on setting up free web servers. In 20:1 Toby complemented this article. Like them I also decided to set up my own ftp server. I did it all completely free and with no hassle. My FTP server was set up on Windows 2000 Professional. I'm also going to give a possible solution to the dynamic DNS problem.

My Hardware: U.S Robotics broadband router and an Alcatel speed touch home DSL modem.

I built a computer from all free parts that I managed to pick up along the way. It's an AMD Athlon 333 mhz with 192 MB ram 10/100 NIC and a 7.5 gig HD. Nothing special as you can see! But let me tell you I ran Win 2000 server on this thing no problem.

FTP Software Used: You can download any ftp program. http://www.webattack.com/freeware/server/fwftpserver.shtml has some good ones. I used guildftpd from http://www.guildftpd.com/. It's very easy to use and configure. It also has great IRC tools on it and of course, *it's free!*

Solving the Dynamic DNS Problem

http://www.myserver.org. There, I said it! You sign up free of course then download the myserver.org SW and run it. Simple as that. Because your IP on cable/DSL is often dynamic, myserver constantly updates your IP to translate to the web address you choose. You can set the speed at which you want myserver.org to check for your new static IP. Keep in mind this is all for Windows. You can configure myserver.org to be a web host, and for ftp, VNC, pc anywhere, mail, telnet and IRC. You can also add the MX record. Myserver.org also gives you the option to open alternate ports in case of ISP port blockage.

Router Configuration

Depending on your ISP your FTP port 21 may be blocked. My port 21 is not blocked. I'm using a U.S robotics 4 port broadband router. They go for about $99 Canadian. All you need is two tabs in the router configuration utility "virtual dmz host" and "virtual server." We'll start with virtual dmz host. You'll see something like "IP address of Virtual DMZ host" then the internal IP address of the box you're on and you check off "enable."

Next step you go into the "virtual server" tab. This is where you set the router to redirect traffic through your desired port to the ftp server. It looks something like this:

Private IP	Private Port	IP Type	Public Port
192.168.123.xxx	21	Tcp Udp	21

All you have to do is save your settings and logout. Keep in mind NAT is enabled by default on this type of router. After this you're all set to go! Setting up an ftp server was definitely worthwhile. All my SW and troubleshooting docs are always available.

Shouts to: My parents, markay26, bergo, jazon, karim, Scottie D, and bookman.

Maybe these guys can sue a certain government agency since they had the name first. We'd probably all be better off if they took over the department anyway.

Photo by lentil

Voices

Sensitive Info

Dear 2600:

Do you have anything that you absolutely won't print that *could* be considered in the "hacking" community under a general definition? Such as DoS attacks, P2P networks, etc....

f0urtyfive

We tend to focus on methodology which hopefully will get people thinking in a constructive way. What we won't print are things like passwords or codes to specific machines and/or networks because there's not a whole lot that can be learned from that. However, we most definitely will share default passwords and algorithms. We'll also explain how a system works or has inadequacies. If we start down the road of worrying how people will use certain bits of information, the whole purpose of the magazine will be subverted.

Dear 2600:

What are all of these IP addresses and names on pages 40-45 of 19:4? Don't really want to do much scanning unless they're some sort of foreign ass wipe site. Can you help?

brian

We've said too much as it is. But what exactly would you do if they were "some sort of foreign ass wipe site?"

Handy Tips

Dear 2600:

What do you do if you "lose" your admin password on a Windows XP system? Time to format the hard drive, right? Nopers, just pull out your old Win 2000 CD, boot from that, and enter the recovery console. Strangely, Win XP security settings don't affect Win 2K's recovery console, meaning you have full access to the box. If you don't have a Win 2K disk, try changing C:\WINDOWS\SYSTEM32\CMD.EXE to LOGON.SCR and wait until the logon screensaver comes on, sometime 15-30 minutes, and instead of the screensaver the Command prompt will come up. From either of these all you have to do is grab the password hashes and crack them with your favorite password cracker, like Jack the Ripper or LophtCrack if you can't do your thing from the command line. Neat, huh? Hope this saves some headaches.

Jason Argonaut

Dear 2600:

Thank you for the information provided about the telemarketers - namely what is going on when you answer the phone only to hear a few seconds of silence followed by a telemarketer greeting you. It's just so easy to pick out these calls now. Every time I hear this pregnant pause, I just stay on the line and keep quiet. It's pretty easy to tell when it's a telemarketer (all the sounds from a busy call center in the background). When I determine it's a telemarketer, I just keep quiet until he hangs up. It's brilliant! Thanks so much.

tavdog

Policy

Dear 2600:

I'm currently a senior in graphic design at Otis College of Art and Design in Los Angeles. For my senior thesis project I'm creating an informational anti-DMCA booklet to inform the general public about the DMCA, its effects, and proposed solutions being offered. The booklet will be distributed for free on and off campus. Most copies will be distributed to visitors through the college's senior show.

I'd like to request permission to use in part or whole the article titled "DMCA vs. DMCRA" from *2600*, 19:4. I will credit the author and *2600*.

Gloria

By default, we consider this to be acceptable use. We also ask that people using material from the magazine send us a copy of whatever it is they're putting together.

Dear 2600:

I've been meaning to mention my thoughts about the magazine's article policy. Personally I think one part of the article submission policy is unfair. The part saying that all articles submitted to the mag must not have been submitted anywhere else first. Let me give a little analogy here: it would be much like Coca Cola telling all Coke drinkers that they can only drink their product if they haven't drank Pepsi a day or two before drinking Coke. It's unrealistic to think in the span of about three months (actually, over three months for those buying the mag from Barnes and Noble and other stores) that people will always remember they submitted an article to *2600* that they'd *really* like to submit elsewhere as well, or simply want to be bound by such control freak type policies. As is often said in the mag, in some form or another, the exchange of info is and should be free. Such a policy doesn't exactly encourage such a thing, at least during the excruciatingly long wait to see if an article sent gets printed or is thrown away like so much trash.

One thing I think is pretty much certain. No matter what I or anyone else says, that policy will, of course, not change. That's unfortunate. At least for us article writers it is. And, let's not forget something else here. Every time a copy of the mag is sold or someone subscribes you're making money. Money off of other people's hard work. Therefore, doesn't it stand to reason that with that being the case that it's only fitting and right that you listen a bit if such people voice such opinions as this?

Captain B

Your analogy is a strange one to say the least. But it's flawed for the simple reason that you're conjuring up an absurd restriction placed on consumers and comparing it to the guidelines we ask our writers to abide by. We place absolutely no restriction on who can consume - or read - our magazine. To do so would be insane and self-defeating. But our writers are helping to determine the nature of the magazine and for that we have to insist on a certain level of standards. It's a disservice to our readers to simply reprint information which can be found in other publications or on the Internet. The readers are the people we must ultimately answer to and that is why we make this rather simple stipulation. With relatively few exceptions, the articles we print here have not shown up elsewhere. And after their articles are printed here, writers can do whatever they want with them, unlike most other magazines. Why it's such a big deal that we ask you not give us material that readers may have already seen is difficult to grasp. Since you already seem to have convinced yourself that we're exploiting you, we doubt any answer we give is going to satisfy you. We only hope our readers and future writers see the value of these guidelines.

Dear 2600:

In your 20:1 issue you claim that *2600* is a tool for swatting flies. Well, I have used it to swat mosquitos successfully. Does this constitute a violation of your license agreement? Should I hire a lawyer? Am I going to be sued?

Pi

And we're the ones they call troublemakers.

Dear 2600:

Now that I have had an article published, is there someone that I could send future articles to through a more direct means? I have no problem submitting them like everyone else. I am just blatantly trying to jump the line.

No Name

No line jumping here, sorry. Every submission is judged on its own merits, not the name(s) attached to it. But it was probably wise of you to leave your name off of that question.

Dealing With Opposition

Dear 2600:

Al Jazeera is the cable network in Qatar that has acted as the propaganda mill for Osama, Saddam, and any other Arab with an anti-American story to tell. Ironically, it is owned by the same rich fascist who built us a giant airbase in Qatar so we would protect him from his rough neighbors. Here are the results of some basic reconnaissance: [output of whois lookup deleted].

Spams away!

anonymous

We didn't print this data only because it would have taken up way too much space and it's very easily obtained by simply looking up the owner of the domain.

Even if your facts were accurate - which they are far from - your way of dealing with those you disagree with really stinks. How about providing some intelligent dialogue to back up your argument rather than merely attempting to silence different perspectives (through spam, harassment, denial of service, or whatever else you're willing to engage in)? As you probably know if you've read our pages before, we have some major issues with entities who abuse power and intimidate individuals. But we would never condone an attack that would silence those who disagree with our way of seeing things.

Dear 2600:

I am so glad that you publish your magazine. Especially for poignant editorials such as "Not in Our Name" from the Spring 2003 issue. I feel such an affinity to the concepts and ideas expressed. Especially the importance of the fact that "We may not like the message, we may not agree with it, but if what we allege to stand for is to have any value, we have to do everything possible to ensure it isn't silenced."

I am an idealist but I see some dangerous holes in the above stance. For example, I volunteer for a nonprofit media group that has a public web site where anyone can anonymously post news and anyone can anonymously post comments.

Recently we had a lot of hateful speech and threats of all sorts towards women and men who post to the site. This open board got so full of altered and reposted photographs, violent threats, anti-Semitic comments, anti-gay comments, etc. that many posters felt *physically* in danger and didn't want to use the site anymore. Other concerns such as being dragged into a criminal investigation by the police as well as investigation and monitoring by the government feed my nightmares.

The group decided to post a letter about why we thought this was wrong and removed the open board posting on the website. We all regretted doing this and promised to return the open posting ASAP.

How can these practical concerns be addressed and not silence any message whether we agree with the content or not? Are there any limits? Is true equality exploitable?

Your thoughts would be really helpful.

Brian

You are not silencing anyone by removing the open board posting scheme. You're simply not playing host to opinions you find offensive or destructive by permitting them on your site. We find that sometimes people feel the only way to be fair is to allow everyone to say whatever they want in any forum without any sort of control. All that ensures is complete chaos and the eventual destruction of whatever community has been built.

It's essential to not restrict expression and opinions in our society. But that doesn't mean you have to allow others to destroy what you're trying to do. For instance, if we printed everything that was sent to us, the message of 2600 would soon be lost in a sea of gibberish. Are we denying freedom of speech to those whose words we choose not to print? Not at all - they still have their free-

dom of speech. If their words were made illegal by the government or if they were otherwise silenced, that would be a clear abridgment of their rights which would be of concern to anyone regardless of whether or not they agreed with the speech itself.

All that open board posting does is dilute what it is you want to put out and make it so much easier for hostile forces to shut you down. What you offer is not a finite resource. Others can run their own boards and websites. Now if you were a broadcaster using public airwaves that are most definitely finite, then you would have the obligation to give others access. At least in theory. The way things have gone in our society lately, that freedom has been pretty much bought and sold. But that's another story.

Defining Terms

Dear 2600:

I would like to start off by stating that I am not opposed to what you do as an organization, and if anything I'm more like you than unlike you. While I would never consider myself a "hacker" in the contemporary sense, I do consider myself a "hacker" in the abstract sense: one who enjoys the intellectual challenge of overcoming or circumventing limitations. Just don't think you're being reprimanded by some out-of-touch corporate shill or indoctrinated media affiliate when you read the next few paragraphs.

While taking an interest in the hacker culture and the hacker ethic as a whole, I managed to get my hands on some very old text files (some from the mid 1980's) written by very famous hackers such as The Mentor. One of his titles, entitled as it was received by me "the_mentor's_guide_to_hacking.txt," seemed to imply in its first chapter that hacking primarily concerns itself with gaining mainly unauthorized access to systems and information. The part entitled "The Basics" outlines some specific ground rules for breaching network security. One such outline was "Don't be afraid to be paranoid. Remember, you *are* breaking the law." Here, The Mentor openly admits to breaking the law and goes on to say that "One of the safest places to start your hacking career is on a computer system belonging to a college." One would gather that by A) The Mentor's respectable position in the social hierarchy of hackers, B) the fact that he is widely considered one of the most famous hackers to date, C) the fact that he has openly admitted to breaking the law, as well as directing people to a specific type of network to hack, that the nature of hacking most certainly does involve violating the privacy of others. At least, from the reader's perspective, it is a major aspect of hacking.

While reading 19:3, I saw 2600's response to the first letter in the category "The Hacker Ethic," written by anonymous, where the 2600 staff member was quoted to say that "First off, it's not okay to violate someone's privacy, no matter what you call yourself. Doing this is not, contrary to popular belief, one of the tenets of the hacker world." Reading this quote, in conjunction with the above quotes, generates confusion - which I believe is at the root of hacker misunderstanding in the eyes of the media and mass culture. What can be derived from the above is that either hackers really don't know what they entail as far as their ethic goes, or The Mentor isn't really a hacker. In the last case, whomever wrote the response to the letter was lying in stating that hacker ethic does not involve unauthorized breach of systems.

Another issue I see with the hacker community is that it often blurs the lines between "right" and "wrong," often justifying invasion of privacy as "exploration." Can a hacker be a hacker without breaching security by unauthorized means? I have a hard time believing that. I myself am guilty of snooping around when I shouldn't have, but at least I don't hide behind the safety-veil that it's okay because I'm just "learning." Almost every hacker I know is or has been involved in some form of illegal activity pertaining to technology - not necessarily defrauding a bank account, but adhering more to a network-based breach of personal computer security.

In short, I, as well as the rest of the world, need clarification. Is your supposed pretense of "legitimate hacking" an actuality? Are there really hackers that have not gained unauthorized access to something? Or is it just that - pretense - and it's all just a facade to avoid detection from the media or government? What about the different classifications of hackers, like "white hat" and "black hat" hackers? Am I a hacker if I breach security by unauthorized means? Hell, what *is* your personal definition of the term "hacker"?

I am most curious to understand. I thank you for your time and consideration.

fyrwurxx

We don't see an inconsistency here. The piece you read was dealing with one specific area of hacking which involved unauthorized access to a machine. What we maintain is that such unauthorized access is not an essential part of the hacker world. We learn from it, we theorize about it, but to say that it's something you need to do in order to be a hacker is simply not true. Hacking is figuring out how to achieve an objective through trial and error, questioning, sharing of information, and pure stubbornness. And let's be clear on something else - unauthorized access is not necessarily an invasion of privacy. Oftentimes a true privacy invasion occurs when an insecure system is put online with all kinds of personal data on it. It frequently takes someone using unauthorized access to figure it out and tell the world. And other times unauthorized access and privacy invasion are one and the same. Either way, like we said, privacy invasion is not okay - whether you're a hacker, system administrator, government agent, whatever.

Dear 2600:

It's funny to see 2600 complaining about being associated with those who took down aljazeera.net on their news page. It seems to me if it talks like a duck, sounds like a duck, feels like a duck, it's probably a duck. In other words, when you host mirrors of hacked webpages, publish articles on how to exploit IIS, and advocate hacking websites as a "form of expression," it shouldn't come as a surprise when you are associated with those who do this sort of thing regularly. How is this not blatant hypocrisy? Either these people who hack sites aren't really hackers, or you're lying. But if they're not hackers, why do you call it "hacking" webpages?

Another example centers around some of the articles you publish. Articles that come to mind are "Outsmarting Blockbuster," "A Password Grabbing Attempt," etc. What possible relevance does this have to "protecting privacy" and "preserving security"? Teaching readers how to circumvent late fees is nothing short of stealing. Thinly veiling this as a way to get out of a situation similar to arriving 15 minutes late because your car broke down is inexcusable and irresponsible. In "A Password Grabbing Attempt" one is clearly trying to exploit unaccustomed users' ignorance in an attempt to... grab their password. This is not just pointing out a security hole, it's pointing out a security hole and explaining in very close detail how to exploit it for no justifiable purpose. Pointing out a security hole is much more like your article entitled "The Current State of E-Commerce Security."

I suppose this would be a good time to explain that I don't find all your articles immoral and unjustifiable. The "History of 31337 SP34K" was thoroughly entertaining and a lot of your social commentary rings true to me. The article about setting up a home server was informative, and Comcast's Operation EIPS talking points sheet was relieving and yet haunting at the same time.

The bottom line is you can't keep riding the gray area. Either live up to your supposed ethic of protecting privacy, pointing out security holes, and taking necessary steps to assure they're taken care of, or drop the facade. Dogmatically excusing your explorations as free speech is almost as inane as the government encouraging fellow citizens to look over each other's shoulder for "suspicious activity."

fyrwurxx

We've obviously bothered you a lot for you to write two such letters in the space of a month.

Let's start by getting our facts straight. What happened to aljazeera.net was not something so innocuous as an altered web page that could be fixed with a single command. It was a systematic denial of service attack which had the (in all likelihood intentional) effect of silencing their online presence and cutting off their perspective from the world. It really shouldn't be too difficult (unless you're the mainstream media) to see that such actions have got nothing at all to do with hacking and are, in fact, in direct opposition to the open society and free speech that so many of us value. It's a bit less obvious whether or not those who simply deface web pages should be considered hackers. We think it depends on the motive and the execution. Someone simply running a script written by someone else isn't really doing anything that requires hacker ingenuity. Unfortunately that's how a lot of so called hacked web pages come to be. With commonly available exploits, it's possible for a site to get hacked without a hacker being directly involved. But that doesn't mean that creative hackers aren't still figuring out ways around security.

You may not recognize the value of some of our articles but be assured that there are many who do. While you may see the intent of publishing a particular security weakness as only serving the purpose of someone who wishes to exploit it, it's not that simple. Showing the end result is an important part of disclosing a security weakness. Seeing that end result is often necessary in order for someone to take action to either fix it or prevent similar occurrences. And learning the methodology is a vital part of any sort of hacking and what better way to do this than to see specific examples with as much detail as possible?

We simply do not believe security through obscurity is an effective approach. We will continue to expose security holes by discussing them and demonstrating them. History has proven that this is often the only way to get them to be taken seriously.

Dear 2600:

Like Il269U in 19:4 I too am an avid software pirate. Like him, I tend to buy programs which I actually use. Any program which I feel that I would buy if I could not pirate it, I purchase. Since I got DSL, I have pirated software, music, and movies. Before I started doing this, I owned two CDs, about three movies, and not too many computer programs. When I pirate something, I don't view it as getting the program for free. I view it as an opportunity to see if a product is worth my money before I purchase it. Since I began pirating, I have bought many more movies, CDs, and computer programs than I previously owned. This is one of the reasons I dislike the companies that go after piracy. For some people, such as myself, it increases our purchase of their products. Software piracy also lets me view the competition, so that when I am in a position to purchase software for a company, I can make a good decision. This forces software companies to make a better product, which I view as a good thing. While not all pirates purchase that which they pirate, I happen to think that they should. However, I happen to support piracy since it permits users to fully try a product before purchasing it.

revanant

We'd all be kidding ourselves if we believed that everyone thought the way you did. There are a lot of people interested in just getting stuff for free. But do these people define the marketplace? Do they justify the draconian tactics we've been witnessing? Is the industry (software, music, movies) really in peril? We believe the answer is no to all of these questions. The industry needs to adapt to the times and change its attitude towards consumers. They don't really have a choice on this - any more arrogance on their part and continued alienation of their customer base will ensure their extinction as providers. But the content will continue to thrive.

The Law

Dear 2600:

My roommates and I recently were served with a DMCA and takedown notice. This was from the MPAA to our ISP. Our ISP sent it on to us. Thing is, we've got a static IP, and the IP address in the takedown notice was not ours.

I tracerouted the IP and contacted the person who was the real subject of the notice. Apparently nobody downloaded the files in question. The MPAA's cronies got search results back from a P2P app, and based on the titles in the results served the notice. The person serving made a good point: the files could have been a documentary about the media in question or could have been lists of people who are in a fan club of the media in question. In other words, they could have been anything. So the MPAA had no proof or reason to believe that any infringement happened at all. This was all based on an assumption that the titles of the files meant that the files themselves contained copywritten materials. But no measures were taken to prove that assumption.

Now I'll just skip over the due process issues in this notice and takedown protocol, because we've all gone over it a bazillion times. It just seems as if the MPAA is gambling on the ignorance of normal P2P users. It's using notice and takedown to intimidate people when they can't prove, or at least don't bother to investigate, that any infringement is going on. In short, they're counting on our fear. If this person were to challenge the claim that they were breaking the law, they would win. The MPAA has no evidence and can't prove that any laws were broken.

I may be preaching to the choir when I present the above as a case where the DMCA is being abused. I guess the best thing I can say is that if you get served with a notice and takedown, call a lawyer. The accusations may be on thin ice and you may be able to take the opportunity to fight back. A lawyer would know better than you do what your chances are.

Anyway, I started reading your magazine when I was in the Marines and I felt from the onset that we had something in common: We've both made defending civil rights from domestic enemies a part of our lives. Seems like we have more of those now than any other time in recent memory (yes, W., I'm talking about you). Keep up the good work, you're doing more to protect what our country is than people give you credit for.

Jack

Dear 2600:

How are we supposed to fight all this legal crap that's been going on? It almost seems impossible. Between PATRIOT, DMCA, CBDTPA, super DMCA, and all the other local and state laws that are constantly trying to do away with our constitutional freedoms. It just seems like an endless shit storm and it seems impossible to stay on top of it. And how are we supposed to educate the masses as to the implications of these laws when they are so technical (like the DMCA)?

Magelus

It's not supposed to be easy. That's the challenge we face and it's also the tactic of those who wish to overwhelm us. There is no one place to go for all the answers. There is no authoritative source. But there are plenty of places to go for information and a whole lot of people who are interested. The Internet lends itself to just this sort of thing so we need to use that tool as much as we can. Some of our favorite sources of information include: anti-dmca.org, eff.org, epic.org, and aclu.org. These will lead you to others. And we'll print more good ones as we get them.

Dear 2600:

The FCC has ignored the overwhelming will of the public and done a huge disservice to us all by kowtowing to corporate greed and those with a sociopathic desire for domination - Rupert Murdoch, for example.

I ask other readers to join me in contacting our "representatives" in support of S.1046 (or whatever it develops into as time passes) to reverse the FCC rule change of June 2nd, and asking them to make it clear to the bureaucracies of D.C. that the public interest is meant to outweigh corporate interests as they do their duties as "public servants."

One good way to make contact is to use the website http://causenet.commoncause.org/ to look up and send messages to all your representatives simultaneously. Maybe if we start speaking out on the things that directly and negatively affect us somebody will listen. They certainly will not if we roll over, shut up, and continue to take it from the likes of the RIAA, MPAA, big media, and all the other corporate interests in charge.

Jeremy

It's especially important to be creative when engaging in this sort of thing. One mass-produced letter duplicated endless times will have far less of an effect than individual letters, phone calls, or visits. Don't expect immediate results - the system is designed to frustrate you into thinking that your voice is having no effect. By keeping the pressure on, making your presence known, and having a large number of compatriots, their tactic of ignoring and dismissing the opposition will soon become impossible to sustain.

Dear 2600:

Want to help the students who got sued by the RIAA? They have donation pages set up here: http://www.chewplastic.com/ and http://danielpeng port5.com/. A lot of people on P2P networks might see themselves in this type of situation in the not-too-distant future. You might wonder when they're going to come for you?

KoDo

Letter Responses

Dear 2600:

In response to the letter about Deep Freeze in 19:3, I would like to point out that not only does Deep Freeze "freeze" the hard drive, it also freezes the bios. Therefore if there was a password on the bios you could not get into it and boot from disk, considering that they did not put the floppy to be checked when the machine starts up, making Deep Freeze "unhackable." There is no way around this neat program unless you have a program to get the bios password, which is impossible on my school computers because every bios recovery program I've tried has failed to get the password.

encrypted

Dear 2600:

In regard to several of the letters about Deep Freeze, I have to say I downloaded the trial and it looks like a really great product that has many uses. Its ability to clean up the registry and hard drives of the "frozen" computer, while leaving you the ability to save to "thawed" drive is amazing. I know a few people that I've spoken with in chat rooms and similar places online that used to reboot their entire OS every couple of months so that they could run the Macromedia trial products and similar type downloads all the time without worrying about going over the time limit. With Deep Freeze, they'll now be able to just reboot and start with a clean install anytime that they want to work on something. As long as they save their work to a thawed drive or online somewhere on a server that doesn't have a frozen drive it'll still be there but the product that they used to create the work won't be... interesting. I wonder if Deep Freeze will end up messing with Microsoft's Palladium when it finally is widespread....

Lookat ThatThar

Dear 2600:

This info is in relation to scott's letter in 20:1 about the magazine not scanning correctly. In the bookstore/magazine industry, magazines are rarely entered into the system using an actual price. The reason for this is because quite often magazines vary in price due to special issues and such. The common POS "fix" for this is one of two things. The first (and the most common thing) is to just have a magazine key on the keyboard with a manual price entry. In this method, the cashier just presses the key then enters the price. This happens to be the system that B&N uses. The other way of doing things (rarely used due to lack of support in the POS software used by most bookstores) is to have the UPC for the magazine in the system but have it be open priced so that the cashier scans the magazine, then enters the price.

TC

When the price changes, as we recently found out, a magazine is required to change its UPC to correspond to the new price. The "bipad" number, which is used to actually identify the magazine and which makes up half of the UPC, does not change.

Dear 2600:

Last spring, Eigenvalue asked how to request a cached page be removed from Google's index. The wizards of Google, planning ahead, have made provisions for this. The instructor should publish his answer sheet as HTML (rather than PDF) so that he can use the following. In HTML head, he should add the metatags META NAME = 'ROBOTS' CONTENT = 'NOINDEX, NOARCHIVE'. The NOINDEX value tells bots not to index the page at all, the NOARCHIVE value tells bots not to cache it. Presumably, the prof could just use the latter so that students can still find the solution when it is being served, but no mention of this is made in the literature. Check out http://www.google.com/bot.html for more info.

blanch

Dear 2600:

This is in response to Osiris' letter on hacking a Kodak Picture Maker Kiosk at Sav-On (20:1). While at my local K-Mart I tried to touch the top left and bottom right corners on this machine's screen but it didn't work. I did see an icon that would allow me to perform system administration. When I double tapped this icon it prompted for a password. I tried the usual easy passwords, but no luck. I decided that it had to be something hard and didn't have the time to guess that day. So I proceeded to the checkouts and made a purchase. While double checking the receipt, I noticed the store number (which was four numbers) printed on the top. I put the merchandise in my car and walked back into the store to try this number as the password. *Bingo!* It worked. Over the past week I've tried this at Target and WalMart and it was also successful. After you gain access to the system you can do all the things that Osiris mentioned in the letter, plus change the network settings. I believe that they tabulate what customers do with this machine for marketing purposes over the network (dirt bags). Enjoy!

p3rl_junki3

Dear 2600:

Aaron O. Mouse's letter in 20:1 implies that it's hypocritical for 2600 to run an ad for my zine *Infiltration*, since *2600* stands for goodness and *Infiltration* bills itself as "the zine about going places you're not supposed to go." The editorial reply went the marketplace-ads-don't-necessarily-mirror-our-editorial-stance route, which is valid, but I'd like to suggest that our ethics are not dissimilar.

Infiltration is also about opening people's minds, though in our case it's less about encouraging people to navigate mazes of technology and more about encouraging people to navigate mazes of urban structures. We think urban exploration encourages people to participate in their landscapes, develop deeper bonds with their environment, and create adventure for themselves without commercial consumption. *Infiltration* is about applying the hacker ethic to the real world; we find and poke about in hidden spaces in order to get to know and understand them, and then we share what we find out with others. The "not supposed to" tagline doesn't refer to a violation of some objective universal morality, but to the disapproval of the proverbial man. The zine advocates a firm exploratory code of ethics, condemning destruction, theft, vandalism, and invasion of privacy, and supports the idea that the appropriate people should be notified if one finds something amiss. I don't think urban explorers are morally inferior to computer hackers - we're both motivated by healthy curiosity and we're both willing to circumvent obstacles and take back doors in order to see things someone else has decided we shouldn't see on those occasions when we disagree.

Anyhow, I hope *Infiltration* is true to the spirit of *2600*, as 2600 was certainly its main inspiration.

Ninjalicious

Our response wasn't meant to be at all dismissive of what your magazine stands for. It was simply a statement of our editorial policy with regards to the Marketplace. We find the concept of Urban Exploration a *fascinating one but also one which, like computer hacking, is really misunderstood by the uninformed. Here's a view from one of your readers.*

Dear 2600:

In 20:1, Anon O. Mouse writes to condemn your magazine for printing advertisements for zines that teach people about "going places you're not supposed to go." The particular zine in question is *Infiltration* (www.infiltration.org), a Canadian group with an interest in "urban exploration," aka "UE."

As a reader of *Infiltration* and an urban explorer, I feel that I need to clarify certain things that were mentioned in Mouse's letter. What he and your readers need to understand is that the ethics of UE are as rigid and moral as the ethics of hacking. The motto of UEers worldwide is "take only pictures, leave only footprints." We do not gain access to places with vandalism or theft in mind - we are simply curious observers that desire to see something that the public doesn't get to see. We have a basic respect for whatever site we happen to be exploring, and that means leaving it exactly as we found it. Furthermore, while some fringe UEers occasionally use lockpicks to gain access to wherever they are trying to go, this is the exception rather than the norm. If a door is locked and there is no other way in (such as an open window), most UEers will simply leave the site and perhaps return periodically to see if any new entrances have opened.

We are not vandals and we are not thieves. We are simply interested in places that most people don't know exist.

Urban exploration is a fascinating hobby with a following that is not about to die.

darkism

Dear 2600:

In response to Jon in 20:1 about having to push a pipe down the rails really fast, I wouldn't condone it either, but it seems like it would be easier to get wires with clips and a variable resistor to short the tracks. It's easier to turn the knob faster than to push a pipe down a track.

dhax

Dear 2600:

This letter is in response to the TheTechnophile's letter in 20:1 which was in response to my previous letter regarding the Coinstar network. To be honest, I have never seen nor heard anything about duplicate receipts printing from a Coinstar machine. I do know the following, however. Each Coinstar machine keeps a log of its transactions locally and uploads these logs to the Coinstar Headquarters in Bellevue, Washington each night. It is possible to access these logs on the machine itself. However, two things need to be done before the machine can access such logs: (1) the key to the machine must be obtained and used to open the lower half of the machine and (2) the passcode must be entered on the machine's keypad. I know that many stores keep a surveillance camera on the machine and by showing that your friend did not touch the keypad, you can eliminate the possibility that he printed the receipt himself (someone with access to the passcode would need to have printed it). However, this does not necessary transfer the blame to your friend's manager either. Someone else with the code and key to the machine could have accidentally printed it when trying to troubleshoot the machine and your friend could have picked it up and turned it in, not knowing what it was. The receipt could have been printed as a test after a new roll of receipt tape was inserted into the machine and simply was not removed and destroyed.

If you wanted to make a case for your friend's innocence you would first have to obtain a copy of the receipt he allegedly turned in. Next, you would have to obtain records of when the machine was serviced prior to your friend obtaining the receipt. In addition, a copy of surveillance tape taken when your friend opened the machine would be especially helpful.

While I would again like to emphasize the fact that I have never seen such a receipt, the possibility of a "duplicate" receipt being able to be printed is rather high, though if your friend did not have access to the code for the machine, he would have been unable to print the receipt in the first place. I hope that this information is a help to you.

area_51

Dear 2600:

In response to TimBER's letter in 20:1: in your letter you said that if a call is dispositioned as "Do Not Call," it just removes it from that campaign list. This is actually incorrect, at least at the call center I worked at. We were working from a list that we got from a pretty evil cable company on the east coast. It was actually a list of their customers and we were calling to try to get them to upgrade their cable television service or to try the cable Internet service. If a customer requested to be added to a "Do Not Call" list, you disposition the call as "Do Not Call," which flags the account and the cable company removes the caller from the solicitation list. If you just want to remove the customer from the current campaign, you mark "Not Interested." One other way to remove yourself is to say that you don't speak English and the call will be flagged as "Language Barrier." I was told under no circumstances to try to communicate in another language - something that we could get fired for pretty easily. Just a side note: if you hang up on a telemarketer or tell them that you cannot make that decision, more than likely the call will be dispositioned either as "No Contact" or "DM (Decision Maker) Not Available," in which case the number will be flagged for a call back within a few hours. This is at least accurate with the software that we used (Liberation 6000). Not sure about other brands. You could probably search google for a more detailed explanation of telemarketing software... but that would require typing.

dfecter

Dear 2600:

I am a former sailor from the USS Theodore Roosevelt. I transferred from there during the recent Iraq war. I read the letter from the individual seeking a 2600 meeting onboard. I know quite a few people who I worked with might be interested in such. I forwarded the text of the letter to some people I knew onboard. Hopefully the right people will see it.

Walter

Web Feedback

Dear 2600:

As I got settled into my house after work on April 1st I see "2600.com is now property of the U.S. government." That's not cool. You don't need to scare me like that.

Scared in Iowa

We'll be the judge of that.

Dear 2600:

You've probably gotten a million of these but thumbs up on the April Fool's day website.

demosthenes

Dear 2600:

So I'm sitting here at my computer and looking at your website on April Fools.

Thanks, it's nice to think again.

Talofa, Me in Downey

Dear 2600:

Your website used to be cool. Now it sucks. No matter where I click I always have this feeling of being lost in it. Not much thought was put into the design of it.

Inachu

Considering our site hasn't changed very much in the last few years, perhaps you really are lost in the web. Then again, we do try to promote that lost feeling.

Unlearn

Dear 2600:

Similar to confusedbee's letter in 20:1, the technical institute I attend is actually giving out what it considers "official definitions" of hackers and crackers. In fact, during a review we learned an upcoming test may feature the questions "What is a hacker?" and "What is a cracker?" A hacker being, according to them, someone who plays with computers to learn more about them. The teacher got even more specific, saying a hacker is essentially nothing more than a programmer. A cracker, on the other hand, is someone who uses a computer for destructive purposes (whatever they may be).

So now, virtually everyone in that class believes a hacker can do nothing more than program. Anyone who figures out how to bypass security, or do any number of things you'll find in *2600* is a cracker.

This should demonstrate two points. First, the term "cracker" has no meaning except what people give it, so why even bother? Like *2600* has said so many times, stick with computer criminal, or even better, describe the "crime" that was committed and let people decide for themselves whether it was ethical or not. Second, and perhaps worst of all, the idea that a school is programming students to think a certain way about any group of people sickens me. Even people in the hacker community argue over what exactly a "hacker" is. A teacher has no place giving his opinion as fact.

Screamer Chaotix

Dear 2600:

As a requirement for graduation at my high school, each senior is required to give an 8 to 12 minute speech on the topic of their choice at an assembly in front of the whole school. The speech must be controversial and informative. From the beginning as a young sophomore, I knew I would talk about hacking. As the speech grew closer, I had the perfect topic, one that I felt was very important and controversial and one that I felt very strongly about. After reading your magazine over the years and watching the fabulous *Freedom Downtime* many times, I knew this would be among the best chances I would have to speak out about Kevin and hackers in general to a group who would be uninformed or who had given into the common perception of the criminal hacker. While my other peers painfully wrote their speeches over the year conducting research and writing what was to them simply a long paper, I found my countless hours of research (including *Freedom Downtime*, *2600*, all the great archived *Off The Hook* shows, *Hacker Culture*, John Markoff stories, several *Screen Savers* interviews, etc.) to be quite interesting and I learned so much more about Mitnick that I had not known. The writing of it just came out and before I knew it, I had written 13 pages on the subject. In the end the speech was even a little long rounding out at 15 minutes but there was nothing I could cut - it was all so important. In the beginning I spoke about hackers in general, what they were, traced the history and how they had been demonized. I made a nice slide show full of pictures from kevinmitnick.com and other places and I did my speech for the whole school. In the end, I put www.eff.org on the screen to allow others to go there if they wanted to help in freedom on the Internet. I truly believe the speech went over well. While many people now identified me as a hacker, I think their understanding of hackers was more accurate. Many people congratulated me on my speech, but also many people understood and commented on what an injustice the case of Kevin Mitnick was. I want to thank you at *2600* for the inspiration to write the speech and tell you it is truly wonderful what you did to let others know about Kevin. I simply learned from this and used an opportunity. I hope to continue to let people know about Kevin and others who have been criminalized like him. If Kevin is reading this, I am glad you are now free. At least now we may look back on your case and realize how ridiculous it was, let others know about it, and work to stop the horrible misconceptions about hackers that exist today.

JPK

We congratulate you on your efforts. Only by reaching out to the uninformed can we ever hope to achieve a degree of change. It takes hard work and courage to step into the fray and present the facts. But the feeling that you may have actually made a difference is well worth it.

Dear 2600:

We are eighth grade students attending a school in Queens, New York. As a part of the eighth grade curriculum, we must complete a social studies exit project dealing with one of the problems of New York State. We will be based on a high school level for our school has accelerated programs.

The topic we have chosen to study is that of the dangers of chat rooms. We understand that you are affiliated with this topic. As a necessary component of this project, we must write letters and conduct interviews. We would like to know if you might aid us in our mission by contacting either by e-mail, letters, telephone, or in person to give any information regarding the topic. Specifically, we'd like to know why your organization is supporting chat rooms when it is known that they harbor such dangers.

It is strange that there are still organizations that promote the use of chat rooms as a communicative device after so many incidents have occurred. Why does your company promote them? Especially your company. You are hacking magazine? A magazine that utilizes such dangers to take advantage of children and honest companies? What is the moral behind this? Our group would like to know why you and your company think it is OK to hack and as a result of this, promote the abduction and abuse of innocent adolescents. It would be extremely helpful if you could answer our questions as we are interested in your organization. If you have further information or brochures of any kind, advertisements, please contact us.

Amanda, Camille, Meriam, Christina

And who says that schools these days are propaganda mills?

We appreciate the questions and only wish we had received them before the end of the school year. But it sounds as if you've already made your conclusions and are simply looking for us to fill in the parts about the bad guys.

When exactly did we go around promoting chat rooms anyway? What's all this about taking advantage of "children and honest companies?" And we promote abductions and abuse of adolescents?! Your teacher must have worked for a political campaign to successfully get you to believe such crap without any supporting evidence. Your leaps of logic are a whole lot more accelerated than the program you're in.

We don't enjoy insulting a bunch of eighth grade girls. Not a whole lot anyway. But we feel it's only right to also offer you some advice which is clearly more than you were given in this sorry excuse of a class. When seeking out the facts in a story, seek them before reaching your conclusions. What kind of response do you expect when you make such ridiculous accusations and state them as if they were fact?

Perhaps this was all some subtle way of teaching you of the dangers of prejudging a group of people, in which case your teacher is a genius. We're trying real hard to cling to this possibility.

Random Observations

Dear 2600:

Just saw the new *Matrix: Reloaded* movie today with a group of friends. A few of us had a good chuckle towards the climax of the movie when Trinity (Carrie Anne Moss) comes to use a Panasonic Toughbook with a real Linux-looking command prompt and proceeds to "ssh 10.2.2.2 -l root". She then can be clearly seen hitting enter twice. One thing here is bad and the other is redundant. The bad: Having root allowed to login from remote, even over SSH. And the redundant: the command line shows "#" at the end. On every box I've ever seen, this denotes the prompt as belonging to root, and with every implementation of SSH I've ever used, it attempts to send your local username to the remote server unless specified otherwise. It would have been faster to use "ssh root@10.2.2.2" anyway. Also, for those who don't know the 10.x.x.x address space has been reserved by IANA as subnet address. This seems OK, being as the box was in a foreign location and could have been connected to a local IP network. At least it wasn't something silly like 127.0.0.1.

Upon a second viewing, we saw that she actually used nmap to map out that host and saw that 22 was open, and somehow she knew that it was SSH just by the port. Then she runs "sshnuke," perhaps an in-house hack? I wasn't able to find anything online. The next morning, I was reading my usual slashdot.org/securityfocus.com news, and Kevin Poulsen had written an article in which her hack had been identified as a vulnerability in SSHv1 where a buffer overflow state could occur when a remote user sent large packets to the host. Then a 32 bit representation of the packet length is assigned a 16 bit integer. The resulting difference in data representation causes the 16 bit integer to be set to zero or a really low value.

Then as a result, future malloc() calls that reference to that memory location can be corrupted to an attacker allowing arbitrary code to be inserted into a legitimate process's memory space.

She exploits this vulnerability to somehow shut down power all throughout 27 city blocks. I can't say much more without ruining something. But anyway, I was glad to see a big ticket Hollywood movie portray something involving computers correctly. I would really like to see a fictitious film with a "real" plot about hacking/phreaking/social engineering, etc.

fremont_dslam

It's amazing how many people have commented on this which only proves that people actually do pay attention to the little details. It really adds something when they're somewhat true to reality.

Dear 2600:

I have a few comments to make that I hope readers will take with a grain of salt and consider with a critical mindset. Ahem, a story:

I've been following the Mitnick saga since I started reading *2600* in 1998. Luckily I had the opportunity to see Kevin Mitnick speak at a business convention in Minneapolis a few days ago. I even had the chance to shake his hand afterward and say thanks for coming by. His presentation was, in summary, geared to boost awareness of the threat posed by clever social engineers. I was given free tickets from my employer, so I was doubly happy.

On to the real reason for writing: As I waited in line to meet Kevin afterwards, I saw another guy holding an issue of *2600*, in hopes that Kevin would sign it (he was doing a book signing). I made the mistake of trying to be line-buddies with this fellow. I jokingly initiated the conversation by saying I forgot to bring my issue of *2600* along. He asked if I had been to any of the meetings which I hadn't. He responded that the Minneapolis 2600 meetings haven't been very good for at least a couple of years but he still attends them. I was glad he stuck with it, or so I thought. After a brief period, the guy slid into an endless banter that made my eyes roll back into my head. Talking about his friends "rm rf'ing" Apple Store computers, he used the word "lamas" and "kiddie stuff" a half a dozen times in our two minutes together, probably without even realizing it. Maybe he was excited to run into a fellow reader, but the way he talked about his group's activities seemed grossly egotistical.

Sidenote: Good sir, I'm betting you're going to read this and think I'm a real snooty asshole. There's a chance that I am. I apologize in advance for fingering you (and 2600 Minneapolis) in front of everyone reading, but I had to get this out.

I don't consider myself as being anything special, but I am aware that *2600* aims to be a mildly professional, politically oriented zine that presents a mature mindset. No *2600* readers that I've casually encountered in person have proven this to me. For brief periods, I've had my doubts about *2600*'s presence, as well as its readership, but I've always come back to realize that *2600* is the only organization doing anything worthy in print. Kudos to you. However, some readers I encounter give me the idea that they aren't fully aware of *2600*'s political worth, but are more excited with the shock value associated with hacking. I think about hacking in the sense of experimentation, the mindset, and the tradition of having fun with technology. But hey, others may think differently. I hope that there are other serious readers who can disprove my less-than-positive impressions.

So anyway, given the 30 seconds of my time with Kevin Mitnick, I got the vibe that he was a genuinely nice guy. I mean hey, he had a really good handshake. However, there's irony in the fact that he's Kevin Mitnick, for godsakes... who just preached about the trustworthy appearances of social engineers like himself. So, I'll have to maintain my duties and keep my suspicions.

But in all seriousness, maybe those who meet Kevin in person, or at least those that read about him, will realize that hacking isn't entirely about impressing your friends or showing off to some random dude on the street like myself. Use your knowledge to create, tinker, and do something worthwhile. In my eyes, that's always going to be more impressive than mindless talk.

Weez

We can't really say it any better. Since the hacker world is so open it's not possible to regulate who goes around calling themselves a hacker. If it were possible, then it wouldn't be the hacker world as we know it. And, thanks to the misperceptions of what hackers are about, all kinds of people are drawn in looking for attention and getting it for all the wrong reasons. You will find this in almost any forum where hackers are involved, whether in real life or online. It's unfortunate and a real pain in the ass but it's not worth giving up over. Like almost any culture, a lot of good can be found if you take the trouble to look. And those who have the intelligence and the patience to do this will be amply rewarded with what they find.

Dear 2600:

I happened upon an episode of *Cyberchase* on PBS. It's quite interesting, indeed, because not only is it entertaining to see a crew of whiz kids snowball the enemy, "Hacker," as he is known. What's even funnier, I thought, was the way the show implemented the promotion of creative ways to use math to solve everyday problems (not in the show itself, but in the "extras" like for solving how many jellybeans are in a jar using the ability to calculate volume). For a kid, it was actually neat and interesting stuff, so I have to give them credit there, but I find no connection of that to chasing down hackers, especially in ways which completely disregard and disrespect what a hacker is. That's not the kicker, however, since there is also a portion of the show dedicated to "Cyberchase in real life," as it is called. In this scene, a real person went to go get tickets for a Broadway show, but he realized that the line was way too long and he would not be able to buy in time. He uses mathematics to discover that, seeing if it takes five minutes to cross one portion of the sidewalk, then it will take 20 minutes to cross four. Frustrated, he decides, in a gross promotion of the movie industry, to see a movie which he feels will render better results in line *and* give him the opportunity to see a better show. I have two questions: How does this all relate to the actual showing of chasing down hackers, and why is the MPAA involved in this?

Scott

Dear 2600:

I just finished translating the text underneath "A Glimpse of the Future of Computing" in the table of contents of 20:1. In our changing world I think that you are correct. The center of the world is everywhere. (Or more accurately, nowhere.) As information becomes more freely available through the Internet, in many more places in the world, there really is no central location. I loved seeing the juxtaposition of that particular phrase next to that particular article. Great work, once again.

Sunfist

Dear 2600:

What is the deep philosophical meaning of the cover on issue 20:1? Is Lady Lib R. Tee trying to tell us we are all terrorists (Nicaragua, Guatemala, South America, etc.)? Is she calling for more spooky armed men in the streets of our country? Is she inviting terrorists to spread all over our country? Is she making a cynical statement about the mainstream communication that terrorists are everywhere (look behind you!)? Is she just high and doing one of those weird high-people things? So far I just think that it is some lost scene from *Ghostbusters II*.

Jonathan

continued on page 48

McWireless Exposed

by Epiphany and J0hny_Lightning
j0hnylightning@hotmail.com
epiphany@port7alliance.com

Through word of mouth we heard that select McDonald's locations are offering free Internet access to their customers via 802.11b for a trial period lasting through the 1st of July. This article is a compilation of our findings while playing at several of these Wi-Fi spots. Our exploration was conducted from a laptop running Windows ME and a laptop running FreeBSD 4.8 with Prism II cards.

The Basics

The company that brought Wi-Fi to McDonald's is called Cometa Networks. At the time of this writing, this service is available at only ten locations scattered throughout Manhattan. A map can be found at www.mcdwireless.com. The pilot period will last until July and then people will be forced to pay three dollars for 60 minutes on the network. (Or so they say.) During the pilot period a card resembling a calling card is given out with every meal purchased at a participating Mcdonald's. Each card has a username, password, and serial number in the corner. The username is five characters and the password is five digits. We believe that the two are generated using an algorithm, but we do not have enough cards to find a pattern. Cometa Networks plans to take this project nationwide to hundreds of locations by the end of this year.

The SSID of the McDonald's network is "cometa". Both of the laptops we used connected to the network automatically. Winipcfg and dhclient were used on the Windows and FreeBSD machines respectively to get IP addresses.

Fooling Around

When a web browser was opened on either machine, a DNS error popped up and the browser reverted to login.cometanetworks.com. This site is currently accessible on the WWW, but trying to login causes a cgi error. Before we logged in with the accounts on our cards we wanted to see what was possible. We found that DNS names could not be resolved at all:

```
% ping www.google.com
ping: cannot resolve www.google.com:
  Unknown host
```

However, pinging Google's IP was successful:

```
% ping 216.239.51.99
PING 216.239.51.99 (216.239.51.99):
    56 data bytes
64 bytes from 216.239.51.99: icmp_seq=0
   ttl=48 time=190.319 ms
...
```

Unfortunately, trying to connect to the website by putting the IP of Google in the browser was a bust. So was trying to telnet to any port of any machine's IP address. The next thing we did was change the IP of the DNS servers to that of our local ISP. On *nix this can be done by editing /etc/resolv.conf. On Windows you can change this setting in control panel -> network. Now our boxes were able to resolve hosts. Pinging Google was a success, however trying to view a web page was not. The browser was still directed to the login page. Our boxes were not able to make any TCP or UDP connections to any boxes on the web at all. Telneting or SSHing to a shell account was also a bust. We deduced that TCP/UDP was firewalled, but ICMP wasn't. It was time to log in and work from there.

After putting in a login/password a questionnaire pops up. The HTML on this page had some interesting JavaScript that was in charge of opening the login timer. Unfortunately, changing this code did nothing except cause an error. At a later trial we found that changing the DNS is beneficial, because the default setting causes errors from time to time.

60 Minutes FREE
Wireless Internet Access*
Visit www.mcdwireless.com for participating metropolitan New York City McDonald's locations
Cometa

We kept the BSD machine logged in legitimately and used the Windows box to see what information we could uncover without logging in. After some attempts at pilfering we discovered some interesting HTML code. The suspicious code was this particular string:

```
<INPUT type=hiddenvalue=12
   .103.97.40name=UIP>
```

With a quick portscan using nmap for BSD and SuperScan for Windows we came up with several unusual port numbers. It was one of these that brought us to a discovery. It turned out that connecting to port 1111 through a browser, (http://12.103.97.40:1111), brings up a totally different login page. We have dubbed this "The Back Door." We think this page was set up for technicians who are too busy to be limited to 60 minutes. This IP address also has port 80 open, with a similar "backdoor" login page, except there are some subtle differences in the HTML. A curious traceroute on 12.103.97.40 showed that this was the first and *only* hop, meaning that logging in like this was local to the network of the particular McDonald's we were in. We believe that other locations have similar backdoors which in theory can be found with traceroute and a port scanner. (Just search all the hops for 1111 and you may get lucky.)

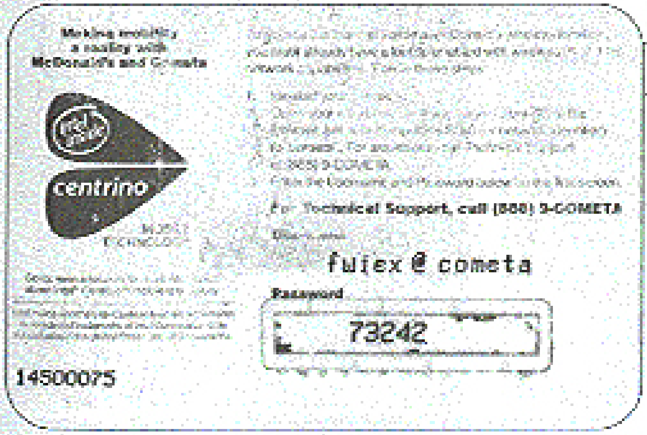
Logging in through the backdoor allowed our computers to connect to the network but without loading up the 60 minute timer nuisance. To test the actual validity of our backdoor, we waited for one of our accounts to expire and tried to login with the same account legitimately. This caused an error. The backdoor worked without a hitch. This only verified our belief that it is possible that the username/password pairs on the cards are algorithmically generated and the local backdoor is not updated with the expired accounts. With the backdoor one account is enough to come back forever and stay logged in as long as you want. Before we left our McWireless exploitation marathon, we slapped a sticker on the wall that said 'Hackers always come in the backdoor.'

Wrapping Up

If there is anyone out there who has played with wireless at McDonald's, we would love to hear from you. We are planning a follow up article for when the pilot period is over and the service is no longer free. And of course, we wouldn't leave you without giving you some logins for the backdoor.

cvktd/57517
fkzdi/42587
uextu/11833
xiiub/71958

Shouts and thanks:
everyone at port7alliance.com, usystems.tk, #mabell, stankdawg.com, MADcow.



Making mobility a reality with McDonald's and Cometa
centrino
For Technical Support, call (888) 9-COMETA
fulex @ cometa
Password
73242
14500075

802.11b Reception Tricks

by ddShelby

Since the article "Comprehensive Guide to 802.11b" in 19:2, I dove headfirst into wireless. I would like to acknowledge Dragorn for a well-written article. I also would like to acknowledge oreillynet.com, seattlewireless.com, and turnpoint.net for the information contained in this article.

Supposedly because of a dispute with Time Warner and the landlord, a cable Internet connection is not available in the apartment building in which I live. DSL is available but seemed a bit steep at $70 a month for a 128K line. So I considered wireless. However, nycwireless.net nodes on the Upper East Side of Manhattan are few and far between and my rather anemic Netgear wireless can't reach the nearest node.

So I looked around for an 802.11b card that has provisions for an external antenna and settled on the Lucent Orinoco Silver. It's a 40-bit WEP card only but it was cheap on Ebay, so to me it did not matter. I picked up a four foot pigtail cable that adapts the connector on the Orinoco card to an N male connector from fabcorp.net

Some Connector Basics

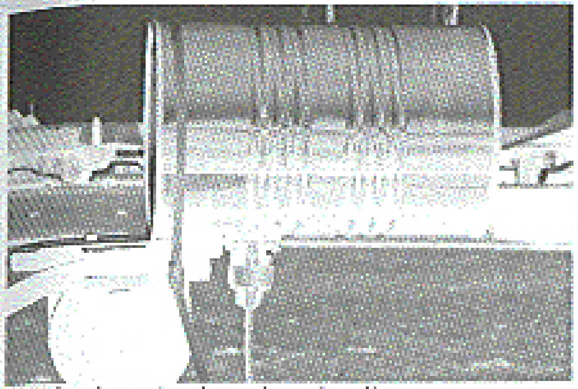
There are several types of connectors used in the 802.11 world that need mention. The most common is the N-connector. These are usually found on the antennas themselves and it seems that this is the norm. The antennas I have come across thus far are all equipped with a female N. The other side of the cable (pigtail) has the connector that will attach to whatever device you are connecting to. Here is where it can get a bit hairy.

Devices like access points or wireless bridges can come with a BNC-, TNC-, or an SMA connector. Connectors on the WiFi NIC's depend on the model and manufacturer of the card. To complicate things just a bit, all of these connectors are available in reverse polarity. Simply put, the small gold pin in the center of a BNC is a male pin. On a reverse polarity BNC, the gold pin is female. The reverse polarity connectors are usually indicated as an RP BNC for example. Just for reference, BNC is an acronym for British Naval Connector, TNC is a Threaded BNC, and SMA is Subminiature type-A connector. All of these connectors, I suspect, originate from the military.

A search on Google revealed a few sites with information on antennas for 802.11b. O'Reilly had the most extensive information I could find (www.oreillynet.com) and is a great place to start if you're new to this like I was.

My first antenna was the famous Pringles Yagi. I constructed it exactly as laid out on the http://www.oreillynet.com/cs/weblog/view/wlg/448 web site and found significant gains as compared to the Orinoco card without any external antenna. A total gain of 11 dbm was the best I could do with the addition of a Pringles can as compared to the Orinoco card itself.

The other antenna choice is the wave-guide antenna. The construction of the wave-guide is easier since it does not involve the use of a threaded rod and washers as the Yagi does. The can itself and the addition of an N connector with a piece of copper wire is all that's needed. For the copper wire I used a piece of grounding wire from common household electrical wire. With the simplicity of the wave-guide construction, you can sacrifice many coffee cans at no significant cost, especially if you're a caffeine nut like myself. The ideal wave-guide antenna for 2.4 GHz is about a 3.25 inch diameter and just shy of 10 inches long. Good luck trying to find those dimensions in a coffee can or anything for that matter on the grocery store shelf. But this being said, there is no harm in experimenting with what you have lying around the house. I first tried an 11 ounce Maxwell House can. I mounted the N connector accordingly at one quarter wavelength from the back of the can as calculated by the handy script located at http://www.turnpoint.net/wireless/cantennahowto.html.



As compared to the Pringles can, the Maxwell House can gave me an additional 3 dbm for a total of 14 dbm. Keep in mind that every 3 db is a doubling of the signal. A loss of 3 db in noise is as good as an overall gain of 3db with respect to the signal to noise ratio. Interesting thing happened though; using Network Stumbler I picked up three more access points that I did not see before. This could be due to the additional gain but I thought it might be the type of antenna construction lending to a wider pattern. So I tried again with a larger diameter can to see if my theory was in fact correct. I chose the Folgers 39 ounce can and cut a hole according to the handy script on turnpoint.net. I reused the N connector from the 11 ounce Maxwell House can to avoid unwanted variables. As it turns out, the gain fell slightly to 13 dbm but I again noticed two additional access points according to Network Stumbler. With the 39 ounce can I now picked up a total of 11 AP's as compared to nine AP's with the 11 ounce can. Of these AP's by the way, four show up in the list printed in the Fall 2002 edition of 2600, and still remain unencrypted. For those of you into warchalking the larger wave guide from a 39 ounce can seems more appropriate than the Pringles Yagi or a wave guide closer to the 3.25 optimal diameter. Although you may prefer something omni directional like a mast antenna, the overall gain is typically lower. So if you are looking for directionality in the signal, then stick with narrow diameter waveguides or Yagis. If broad coverage is what you're after then go with wide diameter waveguides or mast antennas.

Having established the difference in gain and beam pattern associated with the size of the can, I launched a quest for the ideal 3.25 inch diameter can. I needed as much gain as I could get just to reach the nearest nycwireless node closest to my apartment. Blocking that node are three high-rise apartment buildings, two parking garages, countless brownstones, and three blocks. After a near exhaustive search for a 3.25 inch diameter can at 10 inches long, I decided to just spend the dough for a commercial 2.4 GHz antenna. It's a dish style that has an advertised gain of 14 db. The noise on this commercial antenna is slightly lower than any homemade antenna I had constructed, so the overall signal to noise ratio was in my favor by about 3 db. Despite this, the signal to noise ratio was still not enough to get a consistent connection, and dropouts were still too common. So then I thought, do I have to spend even more money for a higher gain dish? Well, not quite.

Dream Cans?

Ah... well, sort of. It certainly looks like the 3.25" x 10" ideal. While shopping for new roller blades at a Sports Authority on Long Island, I noticed a tennis ball can. Most tennis ball cans are now made of the same plastic as soda bottles. But this one is a bit different. Wilson makes an oversized tennis ball for the geriatric crowd, that just so happens to come in a steel can that's 3.25 inches diameter. And the icing on that cake is that the length is just about 10 inches. My three tennis balls were about $6 and the N connector was $2. I punched a hole in the can at 2.49 inches from the bottom and mounted the N connector as the turnpoint.net script calculated. The result was 17 db gain, just enough for what I needed to get a clean signal to the AP. Now 17 db for a tennis ball can is more gain for the money than you might imagine. A commercial antenna at 14 db like the one I bought cost up to $80 and does not include any green fuzzy things to play with. The drawback is that I had to sit near the window with my laptop. My pigtail would only let me stray four feet.

Two Weeks Later

This new Linksys WET11 is neat. The Linksys WET11 is sold as a bridge, not an AP, essentially giving a Cat5 only device the ability to go WiFi or, using two of these WET11's, to connect wirelessly to each other to bridge two wired networks. I got to thinking and wanted to experiment to see what else this thing was good for. I wanted to connect through the WET11 with an AP I already had lying around. So, I picked up a reverse polarity SMA to N male pigtail from fab-corp.com to hook up my Wilson antenna to the WET11. First, the WET11 output is rated at 71mw, which is more than most WIFI cards and more than twice the rated output of my Orinoco

Silver. With an antenna other than the rubber duckie mast provided, there is the potential for some serious range. Also, I wanted to see if I could set up a kind of repeater. So I took the 10 base output from the WET11 and plugged it into my el-cheapo Netgear AP and set the Netgear to a different SSID from the WET11. The results: The Netgear AP worked locally as any AP would, the signal goes to the WET11 via cat5 Xover cable and to the AP that it's aimed at a few blocks away. The connect speed was good enough to give me Internet access in my New York City apartment wirelessly. And with the WET11 sitting on my windowsill and the antenna on the fire escape, I have the ease of surfing from my kitchen table or anywhere in my shoebox apartment without having to contend with the limitations imposed by the four foot pigtail that connects my antenna directly to my Orinoco card. And with the higher output and increased sensitivity of the WET11 versus the Orinoco card, I can use that dish I bought without feeling guilty for spending 80 bucks for it.

Another Wave Guide Idea

There is another design in wave-guides that can pull up to 18 db if constructed carefully. If you take shortcuts or if it's poorly constructed, you can still obtain 13-14 db. The details on its construction can be found at www.seattlewireless.com. It's constructed using a peanut can and some stovepipe fittings from Home Depot. Stovepipe is thin sheet metal and not much different from the material used to make your typical soup can off any supermarket shelf. In this case it's an adapter (sometimes referred to as a reducer) to go from a five inch dia to a four inch dia. This acts to increase the radio waves collected before they enter the can amplifying the overall gain by as much as 6 db. Experimenting with various sizes and lengths can be worthwhile and who knows? You might stumble onto something.

DISTRIBUTED REFLECTIVE

Denial of Service Attacks

by Spyrochaete
http://hyppy.zapto.org

The purpose of this article is to educate those with an interest in Internet security. I wouldn't commit the acts described below and neither should you. Hosting services online costs someone money. Find a more constructive way to express your opinions.

I'm a college student, not a professional (dammit, Jim). Sorry if something I've said is inaccurate. G.I.G.O.

The worldwide Internet is composed of an overlapping array of hardware that directs small fragments of information along various temporary pathways from source to destination. Because of the tremendously high volume of traffic continuously flowing through the virtual veins of the Internet, it is possible for wayward-minded individuals to harness the services of the powerful hardware at the system's logical core without detection, for example, to attack the system of their choice. One such attack that is particularly effective and undetectable by the managers of intermediate communications hardware is the Distributed Reflective Denial of Service (henceforth DRDoS) attack.

DRDoS is the latest in the series of Denial of Service attacks. An explanation of the history of this type of attack is in order to fully understand the ramifications of this new threat.

The standard Denial of Service (DoS) attack is one of the more common attacks by "script kiddies." A properly motivated individual can effectively perform such an attack on the target of their choice with little effort. Denial of Service is the result of local routing hardware being overloaded with fraudulent instructions. Specifically, DoS is the result of exploiting vulnerabilities in the TCP/IP 3-way handshake in which a client and server become aware of each other by swapping synchronization packets. Occasionally an ordinary, legitimate synchronization (SYN) packet will become corrupted causing it to be misinterpreted by the computer on the other end. Servers allow such packets a short grace period before abandoning them. Altering the source IP address of an outgoing SYN packet hides the origin of their source and directs the converse computer to attempt to synchronize with a nonexistent (or unresponsive) host. When this occurs innocently (which it does, regularly and inevitably, however infrequently) the overhead in computing resources is inconsequential and harmless. But when exploited by a malevolent individual, this can be performed by a single computer frequently enough to sufficiently saturate the victim's connection so that its services cease. If the attacker can harness the power of a more powerful machine than the one at his or her disposal, the attack would be that much more effective.

An attack originating from any one machine is not likely to be very powerful or completely incapacitating. Instructing a main router or firewall to ignore IP addresses generating too-frequent packets is a way to terminate such an attack. Although the security system will be bogged down as it examines and discards every unwelcome packet, the network will not be affected by the completion of the packets' journey. By randomizing the spoofed IP address generated in each packet by the attacker, this solution can be invalidated.

The Distributed Denial of Services (DDoS) attack uses the same principal to debilitate its target but is exponentially more effective. The attacker incurs the services of several remote computers ("zombies") by acquiring control over them and issuing simple commands. A common method of secretly achieving control over a computer is to distribute a Trojan virus which installs software that connects the computer to a common server (e.g., IRC) from which the attacker can control a list of zombies en masse like a general commanding infantry. Each zombie simultaneously performs its own DoS attack, saturating the victim greatly and making the process even more difficult to defend against. A properly coordinated DDoS attack can put almost any system at the mercy of an attacker.

DRDoS is a very recent iteration of the DoS attack and is quite ingenious in its design. DRDoS resembles DDoS in that it employs the power of several sources to attack one victim, but it does so in a stealthier, overwhelming manner. In a DRDoS attack, the attacker sends tainted instructional packets to a very large number (hundreds) of innocent clients, alerting them that the victim's computer is requesting a certain service. The very small amount of traffic generated per intermediate attacking server will be so insignificantly small, perhaps smaller than legitimate requests, that it is quite unlikely the attack will be noticed by administrators at all. The astronomical number of service packets (for example, 2 packets per second multiplied by 3000 servers) is sufficient to overwhelm virtually any system anywhere.

One example of a DRDoS attack is the Border Gateway Protocol (BGP) attack. Routers regularly exchange routing tables with their neighbors (routers sharing borders) by asking for and granting permission with each other. In preparation for such an attack, the attacker's first step is to acquire a large list of fast Internet routers. This can be done very easily by performing the IP utility TRACERT on a number of websites and cataloguing, say, the middle five entries. These entries are very likely to be core routers that bridge the huge segments of the Internet. This can be verified by resolving the names of the IP addresses (for example, descriptive FQDNs such as ra1shge34.mt.higpipeinc.com and if-10-0.core1.Chicago3.teleglobe.net obviously represent central routers). An enormous list can be compiled in a few hours automatically via a simple script. The attacker then cycles through the list of routers, sending a sweep of tainted packets stating that the victim is actually a router requesting to exchange routing tables. The sheer volume of incoming packets will incapacitate the victim entirely and immediately until the attacker chooses to terminate the cycle.

This attack, at the moment, is truly impossible for the victim to defend against. It is unfeasible to block the IP addresses of the Internet's major routers because they are required to communicate with valid clients. Because network services are distributed inside the service socket range (ports 1-1023), disabling all communication from these ports may prevent such an attack entirely, but conversely may impede genuine service if the server must occasionally act as a client to fulfill its regular duties. In fact, the only viable solution to this (and many other) attacks lies with Internet service providers who have the power to prevent packets with spoofed IPs from leaving the confines of their services. Unfortunately, the majority of ISPs do not employ this function.

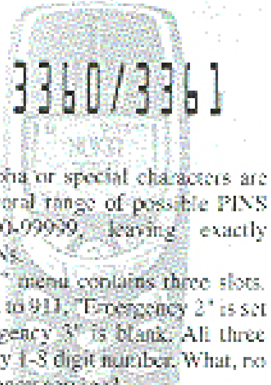
DRDoS is a very damaging, very real concern for the networked world and should not be taken lightly. It is the responsibility of every network administrator to be diligent in preventing their own domains from taking part in such an attack. Auditing a network's activity and employing diligence, education, and insight are all essential to keep one's site secure.

Shouts to: nsmitten, lord_nikon, axiom dadak, purple motion, skaven, necros, mental floss, and efnet #2600 before it got taken over by hackers.

Works Cited

http://grc.com
http://www.webopedia.com
Jamsa, Kris, Hacker Proof, Thomson Delmar Learning, Albany, NY 2001

FUN WITH THE NOKIA 3360/3361



by FragSpaz
fragspaz@fragspaz.com

When I first got my Nokia 3361, I was immediately annoyed by the "AT&T" label (alpha tag) permanently displayed while the phone was in standby mode. This article will outline how to change the alpha tag and network settings on the Nokia 3360 and 3361. Also, I will expose the "secure" menu options for what they are: Wide open.

Nokia 3360/3361

The Nokia 3360 and 3361 are, to the best of my knowledge, identical. The 3361 phone is sold exclusively to prepaid customers (no contract). The 3360 can be purchased by any AT&T customer willing to sign a contract. My guess is that the label 3361 is simply a way for AT&T and Nokia to identify prepaid customers by model number.

Field Test Mode and Security

The alpha tag can only be changed while in Field Test mode. To enter Field Test mode type *3001#12345# at the main standby menu. This will take you to a menu with the following options: NAM1, NAM2, NAM3, Security, Emergency, SW version, Serial No., Programmed, and Field Test.

NAM1 is where the alpha tag can be changed. Before getting into the details of this option, let's take a look at the other menu options.

The "Security" setting is ironically anything but! The "Security" setting allows the security code to be changed, without verifying the original PIN. The default code is 12345 and is probably the same on all Nokia phones (so as not to confuse those cell phone sales people too much). As far as I can tell there is no way to change the Field Test PIN from the default *3001#12345#. Since entering Field Test mode does not require knowing the security PIN, this effectively leaves the door open for anyone to change the security PIN on any Nokia phone without knowing the original PIN, thus locking out the user from "secure" options such as restricting all incoming and outgoing calls!

Notice the string 12345 appears both in the Field Test mode PIN and as default Security PIN. I was hoping that changing the security code would carry over into changing the Field Test PIN, but no such cigar!

On a final note, the security PIN must be a five digit number, no alpha or special characters are allowed. Thus, the total range of possible PINS range from 00000-99999, leaving exactly 100,000 possible PINs.

The "Emergency" menu contains three slots. "Emergency 1" is set to 911, "Emergency 2" is set to *911, and "Emergency 3" is blank. All three can be changed to any 1-3 digit number. What, no long distance emergency service?

"SW version" lists V 03.06 16-08-02 NPW-1PA.

"Serial No." is, well, the 11 digit serial number. It matches the ESN number on the label below the battery. It cannot be changed.

"Programmed" supposedly contains the date of programming, but my phone had MMYYYY listed. I changed mine to 052003 and learned that once changed it cannot be changed again!

"Field Test" lists a sub-menu with Enabled, Enabled+lights, and Disabled. It is set to Disabled by default. I was unable to do anything different, or detect any differences with Field Test Enabled.

Changing the Alpha Tag and Programming Alternative Networks

Now that we have looked around the main menu, it's time to change the alpha tag. While in Field Test mode, select "NAM1." Here there are several options, including an "Alpha Tag" option. Changing the alpha tag in this menu will *not* affect the alpha tag displayed on the phone screen. Apparently, the default tag "AT&T" is programmed out of reach, even in Field Test mode. We need to go one level deeper by selecting "PSID/RSID lists." This will open up a list of P/RSID slots, numbered 1-5.

These slots allow alternative network settings to be programmed in, which in turn can be selected in the "System" menu later on. Thus, it is possible to program in five separate possible network connections. This is great for maintaining your custom alpha tag when traveling in and out of different areas. Simply set up a P/RSID slot for each geographic area you frequent.

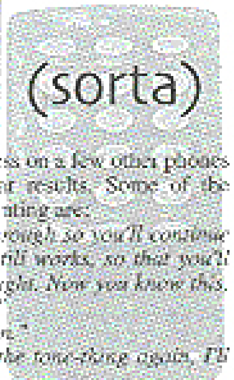
Select a P/RSID slot and we get to the area where an alternative network can be set up. Here you will have to enter a PSID/RSID value (also known as Home System ID), usually a 5 digit number, a Connected System ID, a 3-4 digit value, an Operator (SOC) value, as well as a country code. The SOC value appears to be 2049 in all U.S. AT&T service areas and the U.S. country code is 310. The P/RSID and Connected System ID differ from area to area. To find the P/RSID (Home Sys ID), Connected Sys ID, and SOC in your area, you'll have to do some info gathering. You could try practicing your voice skillz and see if you can tease it out of your local service provider, or let your fingers guide you through a couple of Google searches. I was unsuccessful in soliciting the info from AT&T, but the info is available on the web. I suggest searching Google for "p/sid list" and that should get you on your way.

Once these values have been entered, you are ready to enter your custom alpha tag in the "Alpha Tag" slot. All characters are available when entering your alpha tag. To set the network in effect, reboot the phone by turning it off for a few seconds and turning it back on. There is no other way out of Field Test Mode.

Now it is time to test your new tag and connection. Go to the "System" Menu (Menu 5) and select "Manual." The phone will do a search for available networks. Scroll through the search results of all programmed networks, and if your NAM1/P/RSID info is correct, you will see your custom alpha tag listed as "available." Now back out and select "Automatic" and the 3361/3360 will prioritize your network settings and default to them whenever possible. The only time you will see the "AT&T" Alpha Tag will be when the phone is in an area with really poor reception.

Now take a break and go see *Matrix Reloaded* again.

Why Redboxing Still Works (sorta)



by Plazmatic Shadow
plaz@kevinsnet.com

Everyone says that red boxing doesn't work anymore. I've heard about 40 different explanations for it and I think it's rather annoying. Sure it was one of the "easier," sometimes considered "degrading" forms of phreaking, but it still kept within the limits of the spirit.

Why doesn't it work anymore? For starters, AT&T stopped accepting coins for long distance calls. That's probably the main reason. It doesn't seem to work for local calls either or so I'm beginning to notice.

With all this in mind, I had quite the experience a few months ago. After I read in various places that it didn't work anymore, I ran out and tried it. I dusted off the old tone dialer and popped in some fresh batteries. I went to the nearest payphone, and AT&T no longer accepted coins. I decided to try the old local method of going through a live op, which I had gotten pretty good at.

I dialed up my local Verizon operator and told her I was having trouble with a local coin call. She asked me for the number and told me to deposit my coins. When I finished, she "returned" them and said they didn't go through, asking me to try once more. I went through the process again and this time she said her usual, "One moment while I connect your call."

While she was doing this, I asked her if she was just being nice and putting my call through or if my coins had finally registered. As it turns out, she was just being nice.

I tried the same process on a few other phones in the area, with similar results. Some of the responses I got worth printing are:

"I'm just putting it through so you'll continue to think your little toy still works, so that you'll keep using it and get caught. Now you know this, so I'm going to hang up."

"I'm just a nice person."

"Just this once. Try the tone-thing again, I'll call the police."

"You sound so desperate trying to make a call, and with the phone not working and everything. I thought I'd just help you out."

"You sound like an honest person. I'm putting your call through because I trust you."

"The computer didn't register the tones, but I heard the beep, so I figure you put the money in."

And the most common response was when the call did not go through:

"The coins aren't registering. I'll submit this number for service. Please try another phone, sorry."

The whole point of this is that if you sound innocent, desperate, and/or nice, your call will be put through. It's kind of like social engineering. The red box serves the function of tricking the *operator* into thinking you shoved coins in instead of the *computer.*

Basically, if you're on the line with a half-nice operator, your call will be put through just for trying. So dust off the "old red boxes," get some fresh AAA batteries, and start your calling.

If you have questions, comments, thoughts, or anything else remotely related, I'm interested in hearing them.

continued from page 39

Dear *2600*:

I have found that if you push the up arrow and the select button on a DirecTV receiver, you will gain access to the service/technician's menu. This trick works with the DirecTV models HIRD E11 and HIRD-E25. Happy hacking!

NeuRd

Dear *2600*:

Just wanted to say I love your magazine and learned a lot from it. I stumbled across something very interesting at the gas pump last year. Most of the time I use my credit card when purchasing gas. Well, when the pump asked if I wanted a receipt, I accidentally pressed cancel. I didn't think much of it until a week went by and the transaction never came out of my account. In fact, I was hitting that same gas station for about a year and not a dime was taken from my account. This went on for a year until they caught on and changed the system around. But it's very easy to do. This will only work at the gas pumps that ask if you want a receipt *after* you pump with your credit card. So after I finish filling my tank, I press cancel and off I go. I have found a few other gas stations that do this and still use them to this day. Apparently they can't find out who is taking it or I would've been caught a year ago. But is it my fault they forgot to charge my account? Sure, I could tell them their flaw, but with gas prices these days, let them figure it out. Anyways, I've looked everywhere I can think of about this problem and can't find anything about those pumps and how the transactions work. And it's not just with a certain station - I found a wide variety of stations that have this problem. So, enjoy the free gas while it lasts!

Procyrus

We'll bet your letter will have a big effect on the future of this little security hole. So if you've been feeling guilty about ripping off the oil companies, this could be your redemption. And let's not kid ourselves - doing something like this knowing that you won't be charged is ripping off the seller. You can try and justify it with the high price of gas or U.S. policy in the Gulf or any number of things but it doesn't change that simple fact. You're taking advantage of a stupid software error but it's completely their fault and their responsibility to fix. And you deserve credit for figuring it out and telling the world.

Dear 2600:

I just wanted to let you know about something I found on Amazon.com. It's a subscription to your great publication. There's one problem though. They charge $52.57 ($13.14 an issue) for the subscription. It seems there is a tiny markup on their end of the deal. I realize you probably already know about this seeing as it says editor's comments, but whatever.

J

Actually, we didn't know about this at all. We thank you for bringing it to our attention. So far Amazon has not responded to our inquiries as to what exactly they're up to, nor have they adjusted the price downward based on numerous pieces of feedback sent in by various people. We'll keep you updated.

Dear *2600*:

I subscribe to *2600* and it is a very good publication. I also purchased a copy of the video *Freedom Downtime* which also was extremely good. It is all too easy these days to be critical of others and to forget to offer compliments and appreciation to those who do a good job. So, in these days of anti-terror madness and constitutional rights stomping I want to tell all of you at *2600* job well done and thank you very much for what it is that you guys do so well (educating the public - amongst other things).

Ivan

Thanks - it's always good to hear that we've had some sort of positive influence on people.

Dear *2600*:

Of course after reading the last issue, I decided to see what ports are open on singer.com (we were informed about the guest account to log into their Intranet site). Terminal Service is open and you can connect to their desktop. At least the guest account can't logon to the server, but with access to their Global Directory, there are many usernames there....

I think these guys are inviting intrusion attempts.

anonymous

Dear *2600*:

I was reading the Spring 2003 issue of *2600* on page 23 which contains a copy of a letter sent out from the MPAA regarding "piracy" concerns with the new *Harry Potter* film. The letter contains the phone number of the MPAA Piracy Hotline. Naturally curious, I called this hotline at 1-800-662-6797 on the Sunday evening of Memorial Day weekend. I suppose the Hotline staff was off for this national holiday because I got no answer. The call rang over into a recording (non-intelligent, just a basic recording like you would find on a home answering machine). I was offered several key combinations after the recording, one of which was zero to speak with an operator (instructed only for "west coast law enforcement" to get a certain number but I pressed anyway). An operator was unavailable (another reason that I think the processing center was closed). I was surprised to find more keypad options offered (by "jane" of course), one of which was "4" to access a complete directory of the MPAA employee phone database. I called a second time and didn't press zero this time. The message mailbox was "full."

The way the system worked was that you could type in the first few letters of the employee's last name, press #, and then the system would play a recording of the employee that you typed speaking his or her own name. I tried "nancy" just to see what I could get and I got a recording of a guy saying "MPAA mailroom." Maybe they have someone named Nancy working at the MPAA's mailroom. I was able to press a number to direct dial this extension, as well as a myriad of other options.

I don't know if this is all just because there are no ops on duty at the MPAA Piracy Hotline because of the holiday but I thought you would nonetheless find it interesting that the entire employee phone directory of the MPAA is this easily accessible. I believe this would prove an invaluable asset to those working to prevent the degradation of our freedoms by this organization.

Zen Lunatic

Such systems are actually extremely common in the corporate world. It's very handy in the field of social engineering. Whether such information could be useful in fighting MPAA tactics isn't entirely clear. But full disclosure is almost always a good thing.

Dear *2600*:

A belated thanks for my t-shirt and subscription to 2600 in return for my photo of an Eritrean payphone. I didn't expect anything so I was both surprised and delighted when I received this mystery package from New York. I met a couple of really cool people in London a few weeks ago because I was wearing your t-shirt.

I enjoyed the article "A Dumpster Diving Treasure" by Phantasm in 19:4. Even though it was quite jargon-heavy, this is the kind of thing I would show to someone who had no knowledge of the hacker community. I thought the article summed up really well the hacker attitude. It's all about curiosity and self education and there's nothing malicious about it.

And of course I enjoyed seeing my photo on the back of 20:1.

Eritrea is a country that is well worth visiting if you ever get the opportunity. I spent a few months there and it's the kind of place that gives you hope for the human race. This is a country that won a war against a larger, better armed occupying force by educating its citizens and organizing them into a guerrilla army. The Eritrean government now invests heavily in education and health, while refusing to accept the kind of foreign aid that comes with strings attached. As a visitor, it's easy to see where the cracks might appear, but at the moment they're doing really well and I really hope they reap the benefits of the strongly independent stance they have taken.

I hope that the strongly independent stance that you have taken with your magazine continues to benefit the hacker community and wider society.

Mark Sadler

Dear *2600*:

It may interest you to know of a security flaw I recently observed at my local Walgreens. As of late, Walgreens has been trying to convert its usage of paper applications to an all digital networked system for people to apply for a job. This network can be accessed from home by visiting their corporate website or by using the application kiosk they have set up in-store for applicant use. Yes, this is the classic case of "set up a company computer behind the firewall" deal, but it's much worse in this case.

Almost all of Walgreens' office applications are web-based. Everything from the scheduling to photo-processing uses advanced php to organize the data Walgreens receives. So in this case, walking by the kiosk I noticed that someone had left their application unfinished. There for the public was their name and social security number. Being the nice person I am I went to the kiosk and clicked "save for later" so everyone in the world didn't apply for a credit card using her name. After doing so however, I got to wondering if it would be possible to search the history, hit the back button, and view previously entered data. Sure enough, I was able to get the name, address, social security number, phone number, and various other tidbits of information of the last 100 or so people who used the kiosk to apply for a position.

I notified the manager of the flaw, but he seemed indifferent about it. One employee I talked to stated she knew about it for some time but I don't think the severity of such a flaw really had an impact on her. Since then I've also mailed Walgreens' corporate technical supervisor, but received no response. I thought perhaps a little public awareness would create a sense of urgency to fix this.

Just for fun, give a call to EA's tech support line at 866-543-5435. They have a pretty funny bit about your call being monitored by Big Brother.

Mr. "of Lag"

Economics

Dear *2600*:

OK, here's the story. I walked into Barnes and Noble with enough money for *2600*, a large coffee, and a pack of smokes. I went to get the mag and when I went to pay the chick said "5.50 please." I figured since I'm in Massachusetts it was another tax but she said it wasn't and showed me the cover. So of course I had to choose between my coffee and *2600*. So I got *2600* and a medium coffee. Why the pay hike?

Lamerjoe

It certainly isn't a pay hike, at least not for any of us. The fact is our price has remained the same for the past four years while we've had to deal with rate increases for nearly everything around us. We held off for as long as we could and if we did so any longer, we would find ourselves in the red. Commercial magazines are able to offset expenses with paid advertising, a route we'd prefer not to have to go down.

Dear *2600*:

I have been a reader of *2600* for a couple of years now and have to say that the magazine is awesome. Keep up the great work. Anyways, yesterday I picked up a copy of 20:1 from a local bookstore and realized that the price had gone up since 19:4. What I wanted to know is why the sudden price hike, and why did the Canadian price go up $1, whereas the American price went up only $0.50?

J. Miller

There really isn't a non-sudden way to change the price. The reason for the difference in Canadian price is twofold. First, the Canadian dollar is worth far less than the American dollar. Second, because of the amount of time that has passed since the last price change, the gap between the American and Canadian prices has also widened. (The Canadian price also is slightly higher because of extra charges incurred in distribution from here to there.)

Misconceptions

Dear *2600*:

TwinZero said something in 20:1 about the MPAA and the RIAA needing to look within their ranks to find pirates spreading their material around the net. This is very true. Anyone working in a studio production house or the like can get his or her hands on a digital copy of a film, CD, or anything else. But what the MPAA and its cronies really need to do is think long and hard about how they distribute their films. As someone who knows a lot about running movie theaters, I can tell you this. Distributors and the like are almost clueless half of the time as to what happens with their prints of films after they are done being shown. Technically, either they are supposed to be picked up and shipped off to the distributor, where most of the extra prints are destroyed, or they are shipped to other theaters for showing. But often, the distros leave prints in theaters, which leads to projectionists taking home entire 35mm film prints, or just some dusty cans sitting in a projection room for a long time.

Why do I say all this? Because in the theater/film industry for the past two years there has been a constant argument over whether to begin delivering films to theaters digitally via satellite uplink, etc. The film would be sent from a "secure" server with the film being encoded somewhere along the way. This is really just another sad way to force theater owners into upgrading more equipment, or being accused of being dinosaurs for not going "digital." It is also sad to me, because in my eyes, 35mm always looks better than digital, but that's an opinion. I'm sure it will also save countless CEO's precious cash to buy a new SUV.

Anyone who knows anything about computer security knows that this is a ridiculous idea. While the "industry" has many plans for encrypting the feeds that would be delivered to theaters and then projected, it is entirely possible for anyone, in my mind, to get ahold of one of these feeds and record the information to their HD, etc. I have heard that this process has already been used in Japan and some other countries with alleged success. But if the MPAA wants to cut corners distribution-wise by distributing them digitally, they need to make sure they don't cut corners in the security department, because it does not matter how tight or how sophisticated your security is. If someone is working for the "other side" within your ranks, you have lost all your security.

brian botkiller

Article Clarifications

Dear *2600*:

In my article in 20:1, "Fun with Hosting on Cable/DSL," I mentioned dnsq.org as a "reliable" dynamic IP DNS service. Embarrassingly, they had gone belly-up before my article hit the stands. Dyndns.org is another such service, but sometimes I can't resolve my records that are hosted there. I also mentioned a utility called "Direct Update." This includes a list of other dynamic IP DNS services, but I don't know which ones work well. If anyone out there knows of a good dynamic IP DNS service, please let me know.

Toby

Dear *2600*:

I wanted to respond to Durkcain's article "Hacking QuickAID Internet Stations" in 18:1 (yes, I'm behind in my reading!). I need to note that the kiosk you ran into was really running Atcom software; Atcom purchased QuickATM back around 1998.

I will freely admit that the kiosk you encountered was insecure; Atcom's developers were clearly not hackers. But as the senior developer of the original QuickATM software, I strongly disagree with your conclusion that only "lazy" and "dumb" developers would code for Windows. The QuickATM software would have given you much more of a challenge!

Want to secure the Windows box? The original software ran on NT4 using NTFS (with strong access controls), and the user account had almost zero rights (via admin tools). A VxD was loaded early in the boot process to disable certain key combinations (Win, etc.) and mouse clicks. The shift keys were also disabled until the software was running.

A second desktop was registered, effectively replacing the standard Windows one. Even if the user had gotten to the real desktop (possible only by crashing the fake one which ignored all input), there were no icons, no "Run" in the start menu, no items under "Programs." No extraneous software (like Winzip) was installed. Obvious things like Explorer were moved into nonstandard locations. Regedit, notepad, command, etc. were simply deleted!

The crippled IE4 was really a VB program using the IE control, with sufficient hooks to disable right clicks and keyboard shortcuts. No downloading of content was allowed, and certain other MIME types were blocked. Only the http/https protocols were allowed. Cookies/history/etc. were all purged between users. Internet access went through a logging proxy server in the hub; kiosks had no direct access. And yes, the proxy server did some content filtering (the airports insisted).

Hardware was locked down fairly well, requiring two separate keys to get to the floppy/CD drives. Notebooks were used so if unplugged (and left so for a few hours) and replugged, the machines wouldn't automatically start up. Plans had been in effect to rewrite the entire HD on every boot (via a bootable CD). And we didn't create any software backdoors, all maintenance had to be done by opening the kiosk. Usage logs were sent out via a write only protocol to a pod server, so if anything happened, we could step back through it.

Now - was it completely secure? No. The easiest way in was to launch the AOL software. Since AOL was constantly sending updates, we couldn't keep up with the number of things we had to disable. There were a few semi-tricky ways to get to an open/save dialog box - and into the system. In the two years the QuickATM software was running, we only found one person who got in (and he kindly reported it).

Why didn't we develop on Linux? AOL/CServe aren't supported, and market research (in 1995) indicated that we would lose about a third of the potential users if we didn't allow them access. Popular browser support for Linux was also behind the curve (at the time, I think Netscape 3 beta was our best choice).

However, choice of language or OS won't stop you from having exploitable bugs. Being hands-down tricky, trapping all possible exceptions, and spending personal time trying to hack your own system - that's the only way to develop quality, zero-defect software. (Well, maybe low-defect....)

Marc Wallace
(currently looking for a job!)

Dear *2600*:

In the newest edition of *2600* you mentioned something in the article "Not In Our Name" about holding down three buttons on an ATM and it would give you $20. I was just curious if this is true or if you were just using an example. If it's possible, then I'd like to learn more. You don't have to flat out tell me, just point me in the right direction.

Firehazard

No, we didn't mean to start a panic. It was a hypothetical example. However, it does explain a lot of the strange behavior we've been seeing at ATMs over the past month or two.

Dear *2600*:

I was a little puzzled by Gr3y t0qu3's article on destroying the data on CDs in 19:4. Why not just break the CD into pieces? Sure, they snap with a bang and tend to send shards everywhere, but that's easy enough to remedy.

Matt

We would guess that it's got something to do with people growing lazy over time and not doing a thorough enough job when breaking the CDs..

Dear *2600*:

I enjoyed Area 51's article on the Coinstar machines. I can confirm for him that they run Windows. I once walked by one while it was rebooting, and the NT 4.0 splashscreen appeared briefly.

Jim

Dear *2600*:

In the IBuySpy Portal Software article I submitted for 20:1 it looks like you printed all of the "<" and ">" characters in the code as "[" and "]" respectively, rendering the code useless unless fixed.

Papa Doc

We apologize for the error which was entirely our fault.

Dear *2600*:

It's been a little while since I have been able to pick up an issue of *2600*. This time I was surprised to find an article on the Kroger 802.11b network, mainly because I use it every day. Here are some corrections to Kairi's understanding of what happens with it and topography. First, the POS terminals mostly don't use the 802.11b much. The only reason he saw them is the entire store is one node. They use the cat 5 running up into the ceiling for their normal operations.

The WEP encrypted network that he found I would guess is the mail exchange server. If you really want to know what happens there, have fun. I know the type of e-mails that come in and out of there. It's fairly boring. Trust me.

Next we have the login he discovered. "...cash register functions, to ordering shelf labels, to entering UPC codes and item names." That's describing the SPAA system. This system is used by the Scan Coordinator for their daily functions. That system I would suggest steering clear of for the most part. It contains a mode that allows a person to enter new items to the system and adjust prices. The main reason I suggest staying mostly clear is that it's one of the ones that will get you into major legal trouble.

On a happier note I'll give you some clues. "clock" brings up the time clock. There is a separate login for ordering items in to the store. "clock," POS services, and e-mail services are normally run from a wired terminal. "clock" is run from a Wyse terminal, along with half of the ordering program. SPAA and the first half of the ordering program are run from a wireless handheld normally. We all use OpenServer. (I've complained about this before.) There is another machine that he didn't mention that runs OS2. This machine is mainly for running diagnostics on the network and running "batch files." This is a set of files that is sent from the main office to quickly change all the prices that need to be changed. They can cause big problems too. (I accidentally ran a large number of files on the wrong day once. Haven't done that again.)

Hope this helps in any explorations and makes it a little safer for you.

Flat Line

Dear *2600*:

Regarding the article I wrote in 20:1, I have to add that at the time I was very confused between the differences in Flex ANI and "real time" ANI. I was wrong about the PRI line information I provided. The long distance charges will not be billed to spoof ANI unless you are using a toll free service that uses Flex ANI instead of "real time" ANI to do the billing. The difference is Flex ANI is the ANI you get when you call an ANAC like 800-555-1140. It isn't, however, the real ANI for the call. The real ANI for the call is in fact the BTN. I have an ANAC for AT&T that reads back "real time" ANI as opposed to Flex ANI like most ANACs do. When I call the AT&T ANAC the BTN is what is read back instead of the spoofed information. Sorry for any confusion.

Lucky225

Dear *2600*:

First off, I'd like to point out an error in Acidus' article on XM in 20:1. The XM satellites do not put out anywhere near 70 megawatts power beaming to earth, not even ERP (Effective Radiated Power). The power I believe is under 1,000 watts, probably a few hundred, to the antennas. The power gain of the antennas may reach 1,000 or greater watts ERP however.

The comparison of a commercial wideband FM transmission of 200 khz bandwidth (analog) and the digital 125 khz bandwidth of XM is like comparing apples and oranges. You can convey much more information digitally in less bandwidth if done properly. Traditional POTS lines were meant to pass a 4 khz voiceband audio, yet we can pass a 16 khz or better worth of analog audio through the POTS lines by sampling the audio, digitizing it, and using digital modulation schemes to get a high data rate over the lines.

I'm going out on a limb here. XM came out after I got locked up, or I'd probably have played with and even prevailed at decoding XM. I believe that the 125 khz (I have not seen the specs yet) bandwidth of the XM channel to be very sufficient to pass near CD, if not CD quality sound. The key thing to remember is what modulation scheme they use to transmit the data. A CD typically is on the high end passing audio frequencies of 22 khz, sampled at 44 khz to accurately record it digitally. Without overhead (I've forgotten the math and science), I think at least 88 khz of bandwidth in an RF channel is needed to pass that audio in digitized form.

As in transferring computer data, the simplest form is binary. However binary is not very efficient. In the old days of the Bell 103 and 212 modems, a tone was sent for Mark (1) and another for Space (0) to transmit the data. This was fine for 300 and 1200 baud line speeds, but going beyond that, a more efficient data modulation scheme was needed. Quadrature Amplitude Modulation (QAM) is used by 9600 baud modems and higher data rates by Quadrature Phase Shift Keying (QPSK). 16 level (16PSK), and other exotic schemes allow for higher bandwidths (data rate) to be passed over a certain bandwidth of RF (Radio Frequency) channels, or analog lines such as POTS.

Then we get into compression. At the analog level, FM stations compress the audio to make it louder. They do this to make their stations stand out when someone scans the FM dial. People tend to stop and listen to the loudest signal that is pleasing to their ears. Digital compression, such as the ones mentioned in the article make the digital stream more efficient to transfer, like zipping a .txt file. You do lose some audio quality with analog or digital compression.

Audio quality off of XM or Sirius will probably never be CD quality as the world is not perfect. A lot of error correcting goes on and of course dropped data blocks. All kinds of things can happen to a radio signal traveling 22K miles. Even CDs are not perfect audio compared to what the artists played onto the master tapes or even what comes off of the master tapes. Ever look at the audio output of a CD player on an oscilloscope? Not perfect sine waves, but jagged ones, but that is an audiophile can of worms.

Acidus did give some food for thought. If I was not locked up I'd be probing the innards of XM and Sirius receivers. I bet the companies are happy to hear that!

Flame away guys, I need the snail mail.

Stormbringer
William K. Smith, 44684-083
FCI Cumberland, Unit A-1
P.O. Box 1000
Cumberland, MD 21501

Clearing Blockages

Dear *2600*:

I have heard many people complaining about a URL being blocked by their school or some other place. To get around this is fairly simple: free anonymous public proxy servers. This works in my school, but I don't know about others. I would imagine the same thing would work.

One I happen to like is http://www.triumphpc.com/cgi-bin/nph-proxy.cgi.

I used it all the time and can use the net without the "Violation of Terms of Service" crap my school likes to display when trying to visit sites, some of which are even school related.

Just search for proxy servers on the net and if your school blocks the one you use, find another. There are thousands.

Skuzz

Dear *2600*:

I noticed there were a lot of letters sent in complaining about the filtering software at schools, etc. And while the altavista method does work most of the time (in my experience anyway) I've come across a better method.

A nifty little CGI script called CGIProxy (http://www.jmarshall.com/tools/cgiproxy/) allows you to browse indirectly, so the filtering software is never asked if it's okay for you to visit a particular site. All you have to do is load the script onto a webserver and call it when you want to visit a filtered site. It won't, however, be able to get into https:// locations like Hotmail, unless it's installed on an https:// location itself. Once you have it installed and run it, you just type the site you wish to visit in the form. You can also customize your browsing experience through the little checkboxes below the form, which allow you to disable cookies, scripts, ads, or referrer information. This little script will even allow you to browse anonymously and works with all (to my knowledge) filtering software. I've even heard it'll work for people in China.

There are instructions on PeaceFire (www.peacefire.org/circumventor/simple-circumventor-instructions.html) for setting your home computer up as a web server using this method, which includes installing SSL so it should let you into your Hotmail account, etc.

If you install this on a webserver, I strongly urge you to put a password on it, or at least change the name from "nph-proxy.cgi" to something like "nph-87s6df.cgi" to avoid it's being used for anonymous attacks.

Bullet

Dear *2600*:

This is in regards to "2600 Reader" in issue 20:1 who was having a problem downloading *Off The Hook* due to their school's proxy. This pisses me off. I also have Internet filtering software (websense - www.websense.com) that blocks 2600.com among other sites at my office. I understand how frustrating this can be, especially when you want something a little stimulating. So here is one of many solutions. There is a good chance your IS department hasn't blocked websites that allow you to tunnel through to blocked websites using 128 bit SSL encryption. One of my favorites is https://www.megaproxy.com/ secure/. This site requires no additional software or active x controls to be downloaded and works great. You can read more in detail on the site as I want to keep this short. Hopefully this helps, and if it's already blocked there are many sites of this nature. You just have to look (maybe google - that's where I found this site).

Logix

XPloiting XP

www.disinformated.org

by Bill Melater
retaleMIliB@hotmail.com

Remember the old days when a good way to get the latest software was to get a group together to buy it and then make copies for everyone? You thought M$ killed that with their one-activation-per license scheme for the XP suite, didn't you?

Don't they wish. In this article the author will show a realistic way that the average user can, with the aid of good peer-to-peer file sharing software and a CD writer, create copies of Windows XP Professional Edition that act just like the genuine article. The information presented in this article is presented only to show the weaknesses of Microsoft's latest copy prevention scheme. Do not come crying to the author if you use this information inappropriately and a massive horde of gray-suited attorneys descends upon you and pick your bones clean.

First a little background on Windows XP, which comes in many forms. The Professional Edition comes in (at least) these flavors: Academic for students, MSDN for developers and consultants, Retail for average consumers, Branded OEM for major computer makers like Dell and Gateway, Unbranded OEM for small computer makers, and Volume License (or "Corporate") for companies that buy hundreds or thousands of copies at a time to distribute across their enterprises. All the various editions need a product key in order to be installed and activated; we've all seen that little yellow label on the back of an M$ product with five groups of five characters.

Most of the flavors of XP require the installer to contact M$ for permission to use the software - the infamous "product activation" step of the install. When you activate Windows XP you send them a long number and they send you a long number in return. The long number you send them is generated by doing some math on the CD key as well as some generalized information about your computer (no, they can't identify your individual machine). The long number they send you is called the Activation Key. Previous to the release of Service Pack 1 for Windows XP, one could activate a copy of Windows XP Pro by using a key generator (e.g. the famous Blue List key gen) to generate a product key and walking through the activation process just like you had the little yellow label. However, after Service Pack 1 was released, M$ began validating the product keys submitted for activation against a database of all the product keys that had actually been shipped to resellers, and it became impossible to use a fake key to activate most copies of Windows XP.

There are, however, two flavors of Windows XP that do not require the installer to activate. One is the Branded OEM flavor, which often comes pre-installed and pre-activated on various mass-market hardware, such as the latest Dell PCs. This flavor is not so good if you wanted to install the software on multiple PCs. It often won't recognize hardware other than that which it came with, and most major manufacturers don't even ship a Windows XP CD as such with their machines; they instead merge it with the other bundled software.

The other flavor of XP Pro that doesn't require activation is the Volume License, or Corporate, flavor. The story behind it is that admins at large installations don't want to make 1000 calls to M$ every time they roll out 1000 new PCs. Increasingly, when a user reports a problem with his PC, the admins simply replace all the software on the machine, OS included, to avoid having to do any messy troubleshooting or walk over to the user's desk. The way the installation works for XP Pro Corporate is that the installer enters the Volume License Key and that in itself is enough to install and activate the software - M$ is never contacted. The installation process can then be automated and made invisible to the user, saving the admin a lot of time.

It ought to go without saying that anyone who wants to install Windows XP on multiple PCs wants the Corporate flavor. The problem is that the average Joe simply doesn't have access to a CD that contains the Corporate flavor of Windows XP. But most people know someone who's bought a retail copy, or could find several people who'd be willing to pay for a share of a copy at a local retailer. The trick is making the software available to more than one computer.

Here's the step-by-step guide:

1) Obtain an off-the-shelf copy of Windows XP Pro and copy every file on the CD into a holding directory. This is the easiest, if not the quickest, step. Obviously, you have to be careful to keep the directory structure intact.

2) Obtain the files that are different between the off-the-shelf retail version of Windows XP and the corporate flavor. This is one of the harder steps. There are 11 files that are different between the two flavors of XP:

DPCDLL.DL_
EULA.TXT
NT5INF.CA_
OEMBIOS.BI_
OEMBIOS.CA_
OEMBIOS.DA_
OEMBIOS.SI_
PIDGEN.DLL
SETUPP.INI
SETUPREG.HIV
WIN9XUPG\WIN95UPG.INF

All the files are located in the I386 directory on the Windows XP CD, other than the last one, which is in the WIN9XUPG subdirectory of I386.

The "corporate" versions of these files are not widely available, but they can be had from various peer-to-peer file sharing services, often in a package named corpfiles.something. Sometimes the package will come with handy instructions.

3) Merge the corporate files into the holding directory. You can usually just extract the .ZIP right into your holding directory and the files will go where they should. In order to help me verify that the package actually contained different files than I already had, I extracted mine to a temporary directory, then copied them one by one to their final destinations. Note that not all of these files are absolutely necessary - EULA.TXT, for example, has no bearing at all on whether you can make a copy of the software, except to advise you of how illegal it might be.

4) Download the Service Pack 1 Installer from MS's web site and slipstream it into the holding directory. This step is not necessary if you just want to get a copy of Windows XP. But if you're going to burn it to a CD, why not do it right? Doing this step now will save you the long process of applying SP1 after you install. To slipstream the service pack, execute this command:

XPSP1_EN_X86.EXE -s:C:\HOLD\XPPRO

I assume here that your copy of Service Pack 1 is called XPSP1_EN_X86.EXE (it is if you download it from M$ and don't change the name), and that your file set is in the C:\HOLD\XPPRO directory. You have to supply the complete path for the root directory of your file set or the service pack installer will just copy a huge number of files to a temporary directory and then error out.

5) Add any other files you might think are handy into the holding directory. I made a subdirectory called "Tools" in mine and put all the Power Tools for XP into it, along with the Blue List key generator, a text file that contains a few known good product keys, instructions for making another copy, and any utilities I might need with a fresh install of Windows XP Professional Edition.

The Windows XP install routine does not care if there are additional files on the CD. There is a large file called TXTSETUP.SIF that contains a huge list of every file that the installer knows about and where it will belong when XP is all set up. Any file not listed is ignored by the installer, so feel free to keep other things handy on the disk.

6) Obtain the Blue List key generator for the Windows XP suite and use it to generate a few keys for "Windows XP Corp." This step is also not easy. It could take a few hours of careful searching to finally get this program off the net, or long waits to obtain it with a file sharing service. It is almost fruitless to search for the program by name, but it usually can be found packaged in .ZIP files with names like "Windows XP Crack" or the like. It is a small executable of about 49,000 bytes.

The Blue List key generator (named for the group that produced it) makes one candidate key at a time and then tries to validate it by using an algorithm like the one Microsoft's software uses. The real keys have a limited character set - some letters and numbers are never used in Microsoft product keys - but the key space is still very large (greater than 10^25). Only about five percent of the candidate keys pass the program's test, and only about half of those will be accepted by Windows XP's product key software.

It could take the better part of an hour to generate enough product keys to guarantee success. On my AthlonXP 1700+ it takes about 30 seconds for the program to generate one candidate key.

In the Blue List key generator, pick "WINDOWS XP CORP" from the drop-down. Set the number of keys to generate (i.e., the number of candidates to try) and number of keys to stop after (i.e., the number of keys it finds that it believes to be valid) pretty high. I set each to 100 and ended up with four keys that I could try during the installation.

It's a very good idea if you only have one computer (that is, only one means to generate keys), to generate 10 or 12 keys so that you'll be sure to have at least one that works.

7) Use your favorite burning software to create a bootable CD-ROM using your file set. I used a neat little utility that generates a bootable ISO on the fly and burns it to a CD. You should read at least some of the literature I mention in the Links section so that you have an awareness of what's going on in this step. It is possible to use Nero or any other common CD burn utility that supports making bootable CDs. Be aware, though, that there are certain files that you must have in order to make a bootable CD, and that they don't come with some CD-burning software packages.

8) Install Windows XP Professional Edition, and note that when you're asked for a product key, it's referred to as a "Volume License Key." This step is pretty much sit back, relax, and enjoy the show. Windows XP takes about half an hour to install on a moderately fast system, and much longer on older hardware. It took about 45 minutes on a 750MHz Athlon with 128MB of RAM and about 25 minutes on an AthlonXP 1700+ with 256MB of DDR and a 48x CDROM drive.

One of the nice things about having a bootable CD ROM is that you can install Windows XP onto a completely blank hard drive. Without the bootable CD, Windows XP will want you to already have formatted the hard drive, and if you don't have XP or Windows 2000, you'll have to convert the file system later on from FAT32 to NTFS, if that's what you want to use. With a bootable CD you can format the drive NTFS from the beginning.

Another nice thing you can do is create a plain text file in the I386 directory called WINNT.SIF and put these lines in it:

[UserData]
ProductID=FCKGW-RHQQ2-YXRKT-8TG6W-2B7Q8

Replace the series of characters that starts with FCK with your good product key. Beware doing this before you know for sure that your product key will work, as it could cause you to waste a CD or two. If you have this line, you will not be asked to input the product key during install. This is what admins do to save themselves 25 keystrokes every time they install Windows XP.

Note: Do not attempt to use the above product key. It will not work. Microsoft specifically targeted that key with Service Pack 1, disabling it.

9) Verify that your copy of Windows XP is already activated. There are three ways to do this. The first way is to note that there is no blinking icon in the system tray that indicates your copy isn't activated. Another way is to use the copy of Internet Explorer that comes with Windows XP and visit http://www.windowsupdate.com, which will not offer updates to a copy of Windows XP that is not activated. While you're at it, apply all the security-related updates that are waiting. Even if you don't ever use Internet Explorer, Outlook, or Media Player again, there are many applications that use components of Internet Explorer behind the scenes and therefore share its notorious vulnerability to attack.

The third way to verify your activation status is to execute the command:

C:\windows\system32\oobe\msoobe.exe /a

MSOOBE is the program that determines whether Windows XP is activated and leads you through the activation process if not. Rather than prompting you for your location and beginning the activation process, the resulting window should simply say "Your copy of Windows XP is already activated." I like to run this command every so often, just for the warm, fuzzy feeling I get.

10) Enjoy! But beware of a few things. Normally, changing more than three or four components in a Windows XP computer will cause it to want to be reactivated. If that were the case here, the user most likely would have to find a way around the activation process again. There are several ways to do that. Finding them out I leave as an exercise for the reader.

Bear in mind that the actions described above could be counter to US and international copyright law, and to actually do them could lead to legal trouble. Furthermore, I do not know what will happen to a machine that is running a copy of Windows XP that was obtained by the method described above if MS should beef up their copy-prevention efforts. A lot of people who used the famously leaked product keys to install Windows XP were left out in the cold when Service Pack 1 was released and have not been able to enjoy its benefits. Microsoft would certainly be within their rights to engineer Service Pack 2 to leave everyone with illegitimate copies out in the cold, or even to destroy such software.

Microsoft has for years depended on other large companies for the bulk of its profit and only recently began even to try to rein in the massive amounts of copyright violation that had been going on between individual users. Meanwhile they had to keep their original customer base, the corporations, happy. The beauty of this whole thing is that it is possible to use these huge corporations against each other. Microsoft's dependency on other massive companies has left its newest, most copy-protected software with an Achilles heel that the little guy can XPloit.

Bibliography/Links

http://howto2.nu/bootcd/ is a well-maintained page that describes bootable CDs in detail, and includes the instructions and software the author used to make his CDs bootable.

http://www.licenturion.com/xp/fully-licensed-wpa.txt is an older page that describes the algorithm that Windows XP uses to generate activation keys, and tells why they aren't the enormous threat to privacy that some believe them to be.

http://www.extremetech.com/article2/0,3973,11222,00.asp is the best description of the ins and outs of Windows Product Activation that this author has seen, even though the article predates Service Pack 1.

http://www.microsoft.com/piracy/basics/activation/windowsxpqa1.asp is telling if you read between the lines, and also a good source for "the other side" of the piracy/WPA issue.

Marketplace

Happenings

THE SECOND CHAOS COMMUNICATION CAMP will take place August 7-10, 2003. This "International Hacker Open Air Gathering" will take place near Berlin, Germany. Participants are encouraged to bring computers and tents. For those who don't feel like camping out, various towns (not to mention the city of Berlin) aren't very far away from the campground. The Chaos Communication Camp is the official hacker event of the year that 2600 is affiliated with. (In odd numbered years when there isn't a HOPE conference in New York, we suggest that attendees try something different and become inspired by meeting hackers from other parts of the world. Two years ago we helped to sponsor HAL 2001 in the Netherlands. Next year we're planning on holding our fifth HOPE conference.) For more information on this year's event in Germany, visit the Chaos Communication Camp site at http://www.ccc.de/camp

INTERZONE III. April 2004. Not just another hacker con! Stay tuned to website for more details. www.interz0ne.com (that's a zero!)

DUTCH HACKER MEETINGS. Every second Sunday of the month Klumbo organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the 2600 meetings. We meet around 14:00 (2 pm) in front of the GWK office usually. We hope to see you there! More info can be found at www.klumbo.nl/meetings.html

For Sale

WIRELESS SECURITY PERSPECTIVES. Monthly commercial grade information on wireless security. Learn how to protect your cellular, PCS, 3G, Bluetooth, or WiFi system from 2600 readers. Subscriptions start at $90 per year. Check us out at http://wsp-wireless.com/wsp.html

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key chain/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nitrood Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

TAP/YIPL. The original phreaking and hacking zines! All original back issues on CD-ROM. Only $5 including postage! Write for a free catalog of the best underground CD-ROMS! Whirlwind, Box 8619, Victoria BC, V8W 3S2, Canada.

EXPLOSIVES ARE FUN. But do you really understand the principles behind them? Do you know what makes them tick? The science of explosives is both interesting and fascinating, and now you can easily understand the working mechanics of them when you read *The Preparatory Manual of Explosives*, a new release by Jared B. Ledgard. This is an easy to read book that details nearly every aspect of proper preparation, handling, manufacture, and safety related to explosives. This is college level material that was professionally prepared detailing the preparation of more than 100 high explosives and written in plain English for consumption by the average person. A major emphasis is placed on safe handling and manufacture of the explosive compositions described within. *The Preparatory Manual of Explosives* was copyrighted in July of 2002, is 367 pages in length, has a suggested retail price of $39.95, and is a perfect bound paperback book. For a limited time, you may enjoy free shipping on this title within the USA when purchased through amazon.com (subject to terms and conditions imposed by Amazon's "free super saver" shipping offer). For more information or to place an order, please call 1-800-431-8958 and press option 2 when you hear the main menu, visit www.amazon.com and search for ISBN 0-9722837-0-9 or visit www.americansupply.com/pme2000. Tarrance Supply accepts all major credit cards as well as checks, money orders, and well-concealed cash (not advised) and ships worldwide. *Anyone implying illegal intentions will be denied sale.* We reserve the right to refuse service to any customer at any time.

LEARN LOCK PICKING It's EASY with our book. Our new edition adds lots more interesting material and illustrations. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your 2600 reader price discount.

WEBEZINE, the first and only monthly compilation CD-zine featuring new and popular software, text files, e-books, reviews, tutorials, graphics, videos, music, and more. Please help Webezine to continue and grow by submitting files or links or suggestions to [illegible]@hotmail.com or submit@webezine.com. Anything is accepted. Order yours online at [illegible] or [illegible]@yahoo.com/webezine. Also check out [illegible] for the best prices on hosting, colocation, and web design!

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this rarity! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

IP-BLIND OUTGOING SMTP TUNNEL, suitable for installation behind any web-proxy firewall. $80 per year. Will completely disassociate your outgoing emails from your employer's network. Send check to Tippar, Box 45165, Kansas City, MO 64171. Include a good email address for yourself where we will send you the client half of the software. This is for privacy and sidestepping restrictive corporate communications directives, NOT bulk mail or other TOS violations. Your check will not be deposited until you declare your satisfaction.

WORLD'S FIRST "DIGITAL DRUG." Hackers, get ready to experience the next level in software technology! VoodooMagickBox is a 100% legal and safe way to enter into a drug-like trip. All you need to do is place the clips on your ears and turn the knob on the VoodooMagickBox. It's like nothing you've ever tried! For details and ordering information, visit www.voodoomagickbox.com (money orders and credit cards accepted).

CABLE TV DESCRAMBLERS. New. (2) Each $115 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 4521 Olive, Box 28963-TS, Olivette Sub, Missouri 63132. Email: [illegible]@yahoo.com

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration*, the zine about going places you're not supposed to go, send $2 to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

WWW.PROTECT-ONE.COM. Protect yourself! Everyone has a need to be and feel safe from the outside world. We carry a full line of self defense, security, and surveillance products at low prices. Everything from alarms to mini cameras to telescopic batons to stun guns and more! Check us out, all major credit cards accepted. We ship worldwide!

FREEDOM DOWNTIME, the feature-length 2600 documentary, is now available on video! See the adventure unfold as we try to get to the bottom of the Kevin Mitnick story and prevent a major motion picture from spreading more lies. Available on VHS in NTSC (U.S.) format, 121 minutes. Send $20 to 2600, PO Box 752, Middle Island, NY 11953 or order via our online store at www.2600.com.

Help Wanted

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: [illegible]@yahoo.com. You can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

NEED ASSISTANCE to reverse/recover ASCII text data which are [illegible] compressed/encrypted by some type of commercial program. [illegible] rather large, from 30MB to about 600MB. Using DOS [illegible] engine for retrieval. Please advise if there exists any tools [illegible] available or anyone who may be of help. [illegible]@hotmail.com.

I NEED TO BUILD A HIDDEN CAMERA SYSTEM including [illegible] on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any [illegible] information to [illegible]@yahoo.com, fax (206) 350-0556.

Wanted

THE NEW YORK CITY INDEPENDENT MEDIA CENTER (NYC IMC) is looking for donations to help build an IC server to host its open publishing web site. NYC-IMC (http://nyc.indymedia.org) is an all volunteer collective and is part of a worldwide network of over 100 media centers (http://www.indymedia.org) dedicated to maintaining an open publishing web system covering progressive issues and built using open source technologies. NYC-IMC has outgrown its current server and host and would like to create a robust, rack mountable server that can be collocated with a faster provider. If you can donate time or parts to help build our server, please get in touch with the NYC-IMC Tech Team at imc-nyc-tech@indymedia.org.

SEEKING INFORMATION ABOUT TRACFONE. Looking for technical data concerning the Tracfone network and how it operates, especially information about airtime and the manipulation thereof. I have been working for some time to compile an extensive tutorial about Tracfone and how its service works and I am currently working on the fourth revision. The third revision and quite a little bit of information that I have already discovered on my own can be found at www.[illegible].com in the Scams & Fraud section of the site. Send any information via e-mail to [illegible]. I will not pay for information and you shouldn't want to charge for it because that would be against your hacker ethos. Or something. I am also looking for people to write tutorials and other content on the site as well. Contact [illegible] if you are interested. These will also be unpaid positions.

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it does not work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

WANTED: Help to remove CAP ([illegible] upload and download speed) of SBC DSL line. [illegible]@yahoo.com

Services

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaksen Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, Paypal, or credit card. http://www.kaksen.com/

PAY2SEND.COM is an e-mail forwarding service that only forwards messages from whitelisted contacts or people who pay you to receive from them, using a token-pending identity technique. Sign up via our web page form.

VINTAGE COMPUTER RESOURCES FOR RESEARCH. VintageTech provides a wide variety of computer historical related services for business and academia. We provide: support services for legal firms for computer and software patent litigation and prior art research; props and consulting for movie or film production and photography studios requiring period authentic computers and computer related items; data recovery and conversion from old and obsolete data media to modern media; appraisals of vintage computer items for sale, charitable donation, or insurance valuations; sales brokering of vintage computers and related items; general computer history consulting and research. VintageTech maintains an extensive archive of computers, software, documentation, and an expansive library of computer related books and magazines. Visit us online at http://www.vintagetech.com or call +1 925 294 9000 to learn more about the services we provide.

CREDIT CARDS for those with bad or no credit! Almost everyone approved! If you need assistance with getting a credit card, no matter what your circumstances, try us. Send a SASE for further program details and application. The only cost is a $25 application fee (refunded if not approved) and a $50 processing and membership fee for the first year of membership (not due unless you are issued a credit card), and we can even charge it to your credit card so you don't have to pay it out slowly over time. Subsequent year(s) membership fees are only $35 or less. This is a great way to improve your credit rating and credit worthiness. There are many things you can't do without a credit card such as: rent a car or apartment, purchase a home, activate services such as water, electric, and cable (without LARGE deposits), and nowadays you can't even get a good job without a good credit history. Take control of your credit future today. If you are under 18, please let us know as we have a special program for you too. SEND SASE TO: F.D.R. Company, Division of Financial Freedom, P.O. Box 252067, Lewisville, Texas 75029-2067.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, without big brother looking over their shoulder. We provide highly [illegible] local DoS protection. Our main server is a P4 1.[illegible] ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, sftpd, irssi, etc. Affordable pricing from $5/month, with a 14 day money back guarantee. http://www.reverse.net/

Announcements

THE *FREEDOM DOWNTIME* DVD is now in production. We're still looking for ideas for special features and other fun stuff. And if you'd like to help out by translating our subtitles into another language, please write to us at downtime@2600.com with specific information. Remember - you have to be COMPLETELY fluent in both English and whatever language you want to translate the film into. You must also be able to do this within 30 days of receiving information from us.

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer viruses. The White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.christianhackers.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.

Personals

STORMBRINGER'S 411: Am doing a 262 month federal sentence. Would like to hear from those I've lost contact with. Will correspond with others as well. Write to William K. Smith #44181-083, FCI Cumberland, Unit A-1, P.O. Box 1000, Cumberland, MD 21501.

HACKER IN PRISON for being naughty (again). Known as Alphabits for 15 years. I'm doing time in a minimum security state prison for computer fraud. I'm looking to hear from ANYONE in the free world. Help a fellow hacker out! Any reading material is appreciated. Write to me at: Jeremy Cushing - #[illegible], Centinela State Prison, PO Box 911, Imperial CA 92251. Will reply to all.

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resend it each time. Don't expect to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Autumn issue: 8/1/03.

Meetings

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 6 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Victoria: Eaton Centre food court by A&W.

Manitoba

Winnipeg: Garden City Shopping Center, Center Food Court, adjacent to the A&W restaurant.

New Brunswick

Moncton: In the lounge of Ground Zero Networks, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Hamilton: McMaster University Student Centre, Room 318, 7 pm.

Ottawa: Byward Cafe, 55 Byward Market Square. 6:30 pm.

Toronto: Computer Science Education Facility, 40 St. George Street.

Quebec

Montreal: Bell Amphitheatre, 1000, Gauchetiere Street.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Terninalen at Hovedbanegardens Shopping Center.

ENGLAND

Exeter: At the payphones, Bedford Square. 7 pm.

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 7 pm.

Manchester: The Green Room on Whitworth Street. 7 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Grenoble: McDonald's north of St. Martin d'Heres. 6 pm.

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow Street beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: People's Cafe, Cuba Mall. 5:30 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

Tromsoe: The upper floor at Blaa Rock Cafe. 6 pm.

Trondheim: Rick's Cafe in Nordregate. 6 pm.

POLAND

Stargard Szczecinski: Art Cafe, [illegible] Street. 7 pm.

RUSSIA

Moscow: Burger Queen cafe near TAKSAFON ("Telephone Agency of Russia/Telegraph Agency of Soviet Union") - also known as Nikitskie Vorota.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SLOVAKIA

Bratislava: at Propeler. 6 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

Huntsville: Madison Square Mall in the food court near McDonald's. 7 pm.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tempe: Telephones outside mall entrance to Game Works in the Arizona Mills Mall.

Tucson: Borders in the Park Mall. 7 pm.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

San Diego: Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S. Central Ave. and E. Campbell Ave.

Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

Connecticut

Meriden: Meriden Square Mall food court. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court.

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Borders Books on the corner of Meridian and Washington.

Iowa

Ames: Santa Fe Espresso, 116 Welch Ave.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows.

Marlborough: Solomon Park Mall food court.

Northampton: Javanet Cafe across from Pulaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Springfield: Barnes & Noble on Battlefield across from the mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

Buffalo: Galleria Mall food court.

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court.

Raleigh: Crabtree Valley Mall food court in front of the McDonald's.

Wilmington: Independence Mall food court.

North Dakota

Fargo: Barnes and Noble Cafe on 42nd St.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

Cincinnati: Cody's Cafe, 115 Calhoun St., the back room. 7 pm.

Cleveland (Bedford): Bedford Arabica, 728 Broadway. On Bedford Square (Commons).

Columbus: Convention Center (downtown), south food hall, carpeted payphone area, near entrance north of food court. 7 pm.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Rocco's Cafe, 421 SW 10th Ave., near 10th and Stark.

Pennsylvania

Allentown: Panera Bread on Route 145 (Whitehall).

Philadelphia: 30th Street Station, under Stairwell 7 sign.

Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: The Ugly Mug Coffee Shop, 3408 Poplar Ave Suite 16.

Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston. 7 pm.

Houston: Cafe Nervosa in Galleria 2.

San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 6 pm.

Wisconsin

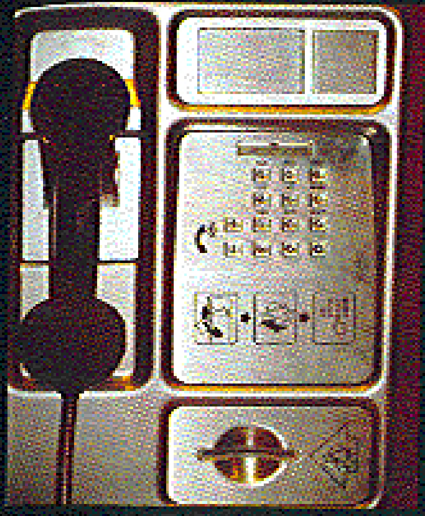
Madison: Union South (227 N. Randall Ave.) on the lower level in the Copper Hearth Lounge.

Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.

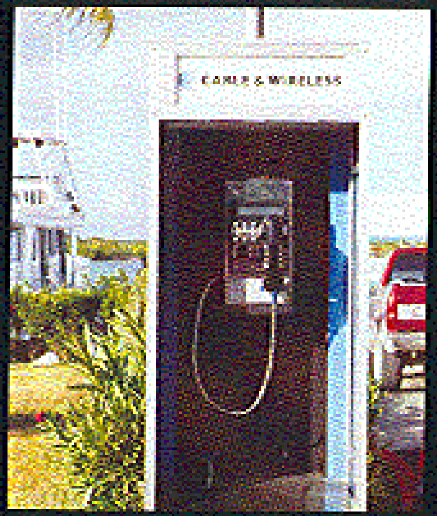
To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Island Payphones



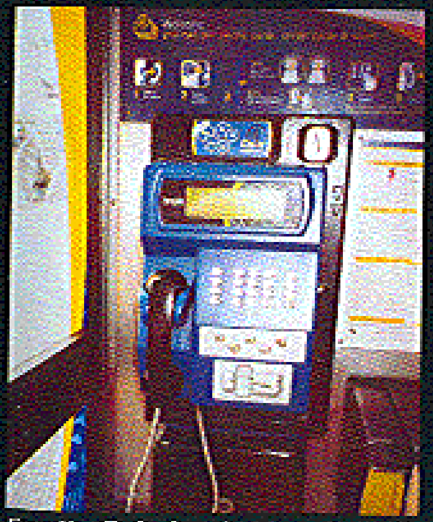
From **Fiji**, this is a charge card phone. Note that Q and Z are represented by the 1 key.

Photo by Zach Andersson

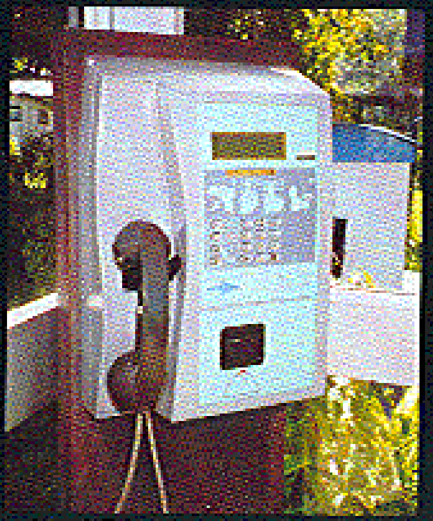


An outdoor booth operated by Cable & Wireless on one of the islands of **Turks & Caicos**.

Photo by nexus-3



From **New Zealand**, a coin and card phone with plenty of documentation and accessories surrounding it.



In **French Polynesia**, this phone was found on an island called Huahine.

Photos by J. Hamilton Davis